ELSEVIER Linear Algebra and its Applications 277 (1998) 149–185

LINEAR ALGEBRA AND ITS APPLICATIONS

Primes in several classes of the positive matrices

G. Picci [a,*], J.M. van den Hof [b], J.H. van Schuppen [b]

[a] *Dipartimento di Elettronica e Informatica, Universitá di Padova, Via Gradenigo 6/a, 35131 Padova, Italy*

[b] *CWI, P.O. Box 94079, 1090 GB Amsterdam, The Netherlands*

Received 12 January 1996; accepted 22 September 1997

Submitted by H. Schneider

Abstract

The classification of primes in the semi-ring of the positive matrices is of interest to control and system theory. A few examples of primes in the positive matrices are known. In this paper results on the classification of primes in the positive matrices, in the doubly stochastic matrices, and in the doubly stochastic circulants are presented.

AMS classification: 15A48; 15A23; 15A51

Keywords: Prime; Positive matrix; Doubly stochastic matrix; Doubly stochastic circulant

1. Introduction

The purpose of this paper is to present results on the classification of primes in several classes of positive matrices.

The motivation of the authors for the study of positive linear algebra lies in problems of the research area of control and system theory. The stochastic realization problem for finite-valued processes, see [21], is of interest to signal processing. In the literature one also speaks of the realization problem for the hidden Markov model, for a partially observed Markov chain, and for a

* Corresponding author. Tel.: +39 49 827 7832; fax: +39 49 827 7826; e-mail: picci@dei.unipd.it.

S0024-3795/98/$19.00
PII: S0024-3795(97)10060-X

finite stochastic system. A positive linear system is a dynamical system as understood in control and system theory in which inputs, states, and outputs take positive values. The realization problem for this class of linear systems is of interest to compartmental analysis and to economics, see for a reference on this class of systems [21]. The main question for these problems is the characterization of minimality for these systems. This question reduces to a problem of positive linear algebra, see [21].

The concept of a prime in the positive matrices has been defined in a paper by Richman and Schneider [22]. The algebraic structure of a semi-ring, in particular that of a monoid with respect to multiplication, allows one to define a prime in the positive matrices. Several examples and special classes of primes in the positive matrices have been published, see [2], Section 3.4 and [22]. Primes in the Boolean matrices were explored in [7]. No complete classification of primes in the positive matrices is known. There is thus a need for such a classification and for the development of the algebraic theory of positive matrices. The use of a classification of these primes for the questions of control and system theory requires further study.

A summary of the results follows. A prime in the positive matrices is shown to be monomially equivalent to the direct sum of an identity matrix and of a fully indecomposable doubly stochastic matrix. The classifications of primes in the doubly stochastic matrices and in the doubly stochastic circulants are subsequently reduced to the classification of solutions of an index equation and of a linear equation over a latin square. The index equation can be solved in a straightforward manner. The linear equation over a latin square requires analytic solvability conditions that grow in complexity with the dimensions of the problem. A procedure to construct all primes in the doubly stochastic matrices is described. Examples of primes in the doubly stochastic matrices are presented, some of which are doubly stochastic circulants.

An outline of the paper follows. The problem of classifying primes and preliminaries are presented in Section 2. The results on the classification of primes in the doubly stochastic circulants, the doubly stochastic matrices, and the positive matrices are presented in Sections 3–5 respectively. Concluding remarks are provided in Section 6. The technical parts of the proofs are collected in appendices. Appendix A contains definitions and results on latin squares and doubly stochastic matrices. The Appendices B and C, contain proofs on the classification of primes in the doubly stochastic circulants and in the doubly stochastic matrices, respectively.

2. Problem formulation

In this section a prime in the positive matrices is defined and the problem of classifying all such primes is posed.

2.1. Terminology and notation

Positive matrices may be regarded as elements of a semi-ring or as representations of convex polyhedral cones. The relationships between the matrix, the algebraic, and the geometric approach is extremely useful. Sources on positive matrices are [2,3,5,17].

In this paper the set $\mathbb{R}_+ = [0, \infty)$ is called the set of *positive real numbers* and $(0, \infty)$ the set of *strictly positive real numbers*. This terminology is used in [9], Section 2.2. Let $\mathbb{Z}_+ = \{1, 2, \ldots\}$ denote the set of the positive integers and $\mathbb{N} = \{0, 1, \ldots\}$ the set of the *natural numbers*. For $n \in \mathbb{Z}_+$ let $\mathbb{Z}_n = \{1, 2, \ldots, n\}$ and $\mathbb{N}_n = \{0, 1, 2, \ldots, n\}$. Denote by $\mathbb{R}_+^n$ the set of n-tuples of the positive real numbers. The tuple $(\mathbb{R}_+, \mathbb{R}_+^n)$ will be called a *vector space* according to the usual definition with the understanding that $\mathbb{R}_+$ does not have an inverse with respect to addition. Denote the *simplex* in $\mathbb{R}_+^n$ by

$$S_+^n = \left\{ x \in \mathbb{R}_+^n \mid \sum_{i=1}^{n} x_i = 1 \right\}.$$

The set $\mathbb{R}_+^{k \times m}$ of matrices over $\mathbb{R}_+$ will be called the set of *positive matrices* of size k by m.

A vector $a \in \mathbb{R}_+^n$ is said to be of *order* k and this is denoted by $n(a) = k$ if exactly k elements of a are strictly positive. The indices of the strictly positive elements of such a vector are denoted by

$$i(a) = (i_1, i_2, \ldots, i_k) \subset \mathbb{Z}_n.$$

The reader is assumed to be familiar with several classes of matrices in $\mathbb{R}_+^{n \times n}$: *permutation matrices*, denoted by $P^{n \times n}$; *diagonal matrices*, denoted by $D_+^{n \times n}$; *strictly positive diagonal matrices* (diagonal matrices with strictly positive elements on the diagonal); *monomial matrices*, denoted by $M_+^{n \times n}$, see [2], p. 67; *doubly stochastic matrices*, denoted by $\mathrm{DS}_+^{n \times n}$, see [17], Ch. V and [14–16,18,20]; *circulants*, see [6,16]; and *doubly stochastic circulants*, denoted by $\mathrm{DSC}_+^{n \times n}$.

If $A \in \mathbb{R}^{n \times n}$ is a circulant then write

$$A = \begin{pmatrix} a_1 & a_n & \ldots & a_2 \\ a_2 & a_1 & & a_3 \\ \vdots & \vdots & \ddots & \vdots \\ a_n & a_{n-1} & \ldots & a_1 \end{pmatrix} = \mathrm{circ}(a), \qquad a = \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} \in \mathbb{R}^n.$$

If $a \in \mathbb{R}_+^n$ then $A = \mathrm{circ}(a) \in \mathbb{R}_+^{n \times n}$ and if $a \in S_+^n$ then $A = \mathrm{circ}(a) \in \mathrm{DS}_+^{n \times n}$. A circulant $A = \mathrm{circ}(a)$ is said to be of *order* k if the vector a is of order k. For $n \in \mathbb{Z}_+$ define the *shift* as the matrix

$$W_n = \begin{pmatrix} 0 & 0 & \dots & 0 & 1 \\ 1 & 0 & \dots & 0 & 0 \\ 0 & 1 & & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & 0 \end{pmatrix} \in \mathbb{R}_+^{n\times n}.$$

The shift W_n corresponds to a cyclic shift by one element of a set with n elements and W_n^k to a shift by k elements. The matrix $A \in \mathbb{R}^{n\times n}$ is a circulant iff there exists a vector $a \in \mathbb{R}^n$ such that

$$A = \sum_{i=1}^{n} a_i W_n^{i-1}. \tag{1}$$

Definition 2.1. The positive matrices $A_1, A_2 \in \mathbb{R}_+^{n\times n}$ are said to be *permutation equivalent* if

$$A_1 = X_1 A_2 X_2 \tag{2}$$

for permutation matrices $X_1, X_2 \in P^{n\times n}$. They are said to be *diagonally equivalent* if in (2) $X_1, X_2 \in D_+^{n\times n}$ are strictly positive diagonal matrices, monomially equivalent if in (2) $X_1, X_2 \in M_+^{n\times n}$ are monomial matrices, and unitary equivalent with respect to a semi-ring if X_1, X_2 are units of the semi-ring. They are said to be cogredient if $A_1 = PA_2P^{-1}$ for a $P \in P^{n\times n}$.

A canonical form with respect to permutation equivalence is known. The reader is assumed to be familiar with the concepts of a *partly decomposable*, *fully indecomposable*, and *totally indecomposable* matrix, see [2], p. 75. It follows from [13] that the set of fully indecomposable doubly stochastic matrices is closed with respect to multiplication.

2.2. Algebraic theory of positive matrices and primes

The algebraic structure of the set of positive matrices is a semi-ring, see [11]. A semi-ring differs from a ring in that it does not have an inverse with respect to addition. Examples of a semi-ring are $\mathbb{R}_+$ and the set of positive matrices $\mathbb{R}_+^{n\times n}$ for any $n \in \mathbb{Z}_+$. For any $n \in \mathbb{Z}_+$ with $n \geqslant 2$ the semi-ring $\mathbb{R}_+^{n\times n}$ is neither commutative with respect to multiplication nor an integral domain.

The concept of a prime can be defined in any semi-ring. Below a definition is stated of a prime in the positive matrices, the doubly stochastic matrices, and the doubly stochastic circulants.

Consider a monoid $(M, ., 1)$. An element $u \in M$ is said to be a *unit* or *invertible* if there exists a $v \in M$ such that $uv = 1 = vu$. Such a v is unique, denoted

by u^{-1}, and said to be the *inverse* of u. Denote by $U \subset M$ the set of units of M. The triple $(U, ., I)$ is a group and said to be the *group of units* of M.

It may be deduced from [2], Section 3.4.3 that if $A \in \mathbb{R}_+^{n\times n}$ then A has an inverse in the positive matrices iff A is a monomial matrix. Thus the group of units in the monoid of positive matrices, $(\mathbb{R}_+^{n\times n}, \times, I)$, is the set of monomial matrices $M_+^{n\times n}$. From this, in turn, it may be deduced that the group of units in the doubly stochastic matrices, $(\mathrm{DS}_+^{n\times n}, \times, I)$, are the permutation matrices $P^{n\times n}$ and the group of units in the doubly stochastic circulants, $(\mathrm{DSC}_+^{n\times n}, \times, I)$, are the shifts $\{W_n^{k-1}, k \in \mathbb{Z}_n\}$.

Definition 2.2. A prime in the set of positive matrices $\mathbb{R}_+^{n\times n}$ is a positive matrix $A \in \mathbb{R}_+^{n\times n}$ such that:
1. A is not a monomial matrix;
2. if $A = BC$ with $B, C \in \mathbb{R}_+^{n\times n}$ then either B or C is a monomial matrix.
Analogously one defines a *prime in the doubly stochastic matrices and a prime in the doubly stochastic circulants*. In the latter definitions the monomial matrices are replaced by the corresponding group of units.

The above definition of a prime in the positive matrices was introduced by Richmann and Schneider [22]. For an exposition on primes in $\mathbb{R}_+^{n\times n}$ see [2], Section 3.4.

Example 2.3. A few examples of primes in the positive matrices are known. In $\mathbb{R}_+^{2\times 2}$ there is no prime. The matrix

$$\begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix} \in \mathbb{R}_+^{3\times 3} \tag{3}$$

is a prime in the positive matrices. In $\mathbb{R}_+^{4\times 4}$ several primes are known such as

$$\begin{pmatrix} 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix}, \quad \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix},$$
$$\begin{pmatrix} 1 & 1 & 5 & 0 \\ 0 & 1 & 1 & 5 \\ 5 & 0 & 1 & 1 \\ 1 & 5 & 0 & 1 \end{pmatrix}. \tag{4}$$

see [22,2], p. 79. There is no classification of all primes in $\mathbb{R}_+^{4\times 4}$.

The problem addressed in this paper can now be formulated.

Problem 2.4. Classify all primes in the positive matrices, in the doubly stochastic matrices, and in the doubly stochastic circulants.

2.3. Solution procedure

In the subsequent sections results are presented on the classification of primes in the doubly stochastic circulants, in the doubly stochastic matrices, and in the positive matrices. The solution procedure for the first two classes is similar and summarized below. The details of the procedures are presented in Appendices B and C.

There follows the description of a procedure consisting of four steps. Application of the procedure to an arbitrary doubly stochastic matrix $A \in \mathrm{DS}_+^{n\times n}$ will yield the conclusion whether or not this matrix is a prime in the doubly stochastic matrices.

First decompose the given matrix by permutation equivalence to the direct sum of one or more fully indecomposable doubly stochastic matrices, see Theorem 4.1. Only if the resulting matrix has the form displayed in (14) can the given matrix be a prime in the doubly stochastic matrices. Attention can then be restricted to fully indecomposable doubly stochastic matrices.

Second, consider a fully indecomposable doubly stochastic matrix $A \in \mathrm{DS}_+^{n\times n}$. It follows from [2], Section 2.5.6 that the matrix has a representation as a convex sum of permutations

$$A = \sum_{i=1}^{n!} a_i P_i. \tag{5}$$

The matrix A being indecomposable implies that the vector $a \in S_+^{n!}$ is of order at least 2. It follows from Lemma C.1 under a condition stated there that A is a prime in the doubly stochastic matrices iff there do not exist $b, c \in S_+^{n!}$ both of order at least 2 such that

$$a = L_m(b)c, \tag{6}$$

where L_m is the latin square induced by multiplication. See Definition A.3 for the definition of this particular latin square. The equivalence follows from the factorization

$$\sum a_i P_i = A = BC = \Big(\sum b_i P_i\Big)\Big(\sum c_i P_i\Big). \tag{7}$$

Third, let $a \in S_+^n$ be of order $\geqslant 2$. It follows from Lemma C.3 that there exist $b, c \in S_+^n$ both of order at least 2 such that (6) holds iff

$$i(a) = \bigcup_{j\in i(c)} i(L_m(b)_{\cdot j}), \tag{8}$$

$$a_r = L_{mr}(b)c_r, \tag{9}$$

where (8) is called an index equation and (9) is called an equation over a Latin square in which $a_r \in S_+^{n(a)}$ contains only the strictly positive components of the vector a.

Fourth, it turns out that the latter two equations can be solved. Solvability of the index equation is tedious but easy. Solvability of the equation over a latin square depends on inequalities having a solution.

The procedure to determine whether a doubly stochastic circulant is a prime in $\mathrm{DSC}_+^{n\times n}$ is similar to that for a prime in $\mathrm{DS}_+^{n\times n}$. The equation corresponding to Eq. (6) is $a = \mathrm{circ}(b)c$.

The historical order of discovery of the results differs from that used for the sections of this paper. Primes in the positive matrices have been analyzed first. The classification of primes in the positive matrices is by Theorem 5.1 reduced to the classification of fully indecomposable doubly stochastic matrices that are primes in the positive matrices. Attention has then been focused on the classification of primes in the doubly stochastic matrices. The latter classification has been reduced to solvability of a linear equation over a doubly stochastic latin square for which a solution procedure has been developed. A particular family of primes in the doubly stochastic matrices, see Theorem 4.2, suggests to consider the classification of primes in the doubly stochastic circulants. This then has lead to the results of Section 3. Subsequently it has been discovered that there are primes in the doubly stochastic matrices that are not circulants and that there is a fully indecomposable doubly stochastic matrix that is a prime in the doubly stochastic matrices but not a prime in the positive matrices.

Remarks on the remaining open problems are stated in Section 6.

3. Primes in the doubly stochastic circulants

In this section results are presented on the classification of primes in the doubly stochastic circulants.

Proposition 3.1. *If $A \in \mathrm{DSC}_+^{n\times n}$ is a prime in the doubly stochastic circulants with $A = \mathrm{circ}(a)$, then $n(a) < n$.*

Proof. This follows from the Propositions B.2 and B.5. □

Theorem 3.2. *Let $A \in \mathrm{DSC}_+^{n\times n}$ be a doubly stochastic circulant of order 2, for $n \geqslant 3$. Then A is a prime in the doubly stochastic circulants.*

Proof. This follows directly from Lemma B.6 and Proposition B.9. □

Corollary 3.3. *Let $A \in \mathrm{DSC}_+^{4\times 4}$ be a doubly stochastic circulant of order 2. Then this matrix is a prime in the doubly stochastic circulants if and only if:*

1. either

$$A = W_4^k \begin{pmatrix} a_1 & 0 & 0 & a_2 \\ a_2 & a_1 & 0 & 0 \\ 0 & a_2 & a_1 & 0 \\ 0 & 0 & a_2 & a_1 \end{pmatrix} W_4^j = W_4^k \operatorname{circ}(a) W_4^j, \qquad a = \begin{pmatrix} a_1 \\ a_2 \\ 0 \\ 0 \end{pmatrix}, \tag{10}$$

where $a \in S_+^4$, $n(a) = 2$, $i(a) = (1,2)$;

2. or

$$A = W_4^k \begin{pmatrix} a_1 & 0 & a_3 & 0 \\ 0 & a_1 & 0 & a_3 \\ a_3 & 0 & a_1 & 0 \\ 0 & a_3 & 0 & a_1 \end{pmatrix} W_4^j = W_4^k \operatorname{circ}(a) W_4^j, \qquad a = \begin{pmatrix} a_1 \\ 0 \\ a_3 \\ 0 \end{pmatrix}, \tag{11}$$

where $a \in S_+^4$, $n(a) = 2$, $i(a) = (1,3)$.

Theorem 3.4. *Let* $A \in \mathrm{DSC}_+^{4\times 4}$ *be a doubly stochastic circulant of order 3. This matrix is a prime in the doubly stochastic circulants if and only if*

$$A = W_4^k \begin{pmatrix} a_1 & 0 & a_3 & a_2 \\ a_2 & a_1 & 0 & a_3 \\ a_3 & a_2 & a_1 & 0 \\ 0 & a_3 & a_2 & a_1 \end{pmatrix} W_4^j = W_4^k \operatorname{circ} \begin{pmatrix} a_1 \\ a_2 \\ a_3 \\ 0 \end{pmatrix} W_4^j, \quad a = \begin{pmatrix} a_1 \\ a_2 \\ a_3 \\ 0 \end{pmatrix}, \tag{12}$$

where $a \in S_+^4$ *and* $a_2^2 < 4a_1a_3$.

Proof. Let $A \in \mathrm{DSC}_+^{4\times 4}$ with $n(a) = 3$ and representation

$$A = \sum a_i W_4^{i-1} = \operatorname{circ}(a).$$

By Lemma B.6, A is a prime in the doubly stochastic circulants if and only if there do not exist $b, c \in S_+^4$ of order at least 2 such that $a = \operatorname{circ}(b)c$. By Proposition B.14 there do not exist such $b, c \in S_+^4$ if and only if $a_2^2 < 4a_1a_3$, since the only possible form of a up to permutation equivalence by a unit is

$$a = \begin{pmatrix} a_1 \\ a_2 \\ a_3 \\ 0 \end{pmatrix} \in S_+^4.$$

Thus Eq. (12) represents the only family of primes in the doubly stochastic circulants of order 3 in $\mathrm{DSC}_+^{4\times 4}$. □

Example 3.5. The matrix

$$A = \frac{1}{3}\begin{pmatrix} 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \end{pmatrix} \in \mathrm{DSC}_{+}^{4\times 4} \tag{13}$$

is a prime in the doubly stochastic circulants. This follows from Example B.13 and Theorem 3.4.

Theorem 3.6. *Let $A \in \mathrm{DSC}_{+}^{5\times 5}$ be a doubly stochastic circulant of order 4. Then this matrix is not a prime in the doubly stochastic circulants.*

Proof. This follows from Lemma B.6 and Proposition B.15. □

The preceding result motivates the conjecture that for $n \in \mathbb{Z}_{+}$, $n \geqslant 6$, and let $A \in \mathrm{DSC}_{+}^{n\times n}$ be of order $n-1$, A is not a prime in the doubly stochastic circulants. Enlarging the size of the matrix but keeping the order 3 or 4 gives the following result.

Proposition 3.7. *Let $A \in \mathrm{DSC}_{+}^{n}$ be a doubly stochastic circulant of order $3 \leqslant n(a) \leqslant 4$, such that*

$$A = W_n^{k-1}\mathrm{circ}\begin{pmatrix} a_1 \\ \vdots \\ a_{n(a)} \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

for some $k \in \mathbb{Z}_n$. Assume $n(a) < n$. A is prime in the doubly stochastic circulants if and only if:

1. $a_2^2 < 4a_1a_3$ *for* $n(a) = 3$;
2. *never for* $n(a) = 4$, $n = 5$;
3. $a_1a_4 > a_2a_3$ *for* $n(a) = 4$, $n \geqslant 6$.

Proof. This follows from Lemma B.6 and Proposition B.16. □

There exist doubly stochastic circulants of order e.g. 3 that are prime, independent of the values of the nonzero elements. An example is $A = \mathrm{circ}(a) \in \mathrm{DSC}_{+}^{9\times 9}$ with

$$a = (a_1 \quad 0 \quad a_3 \quad 0 \quad 0 \quad a_6 \quad 0 \quad 0 \quad 0)^{\mathrm{T}} \in S_+^9,$$
$$a_1 > 0, \quad a_3 > 0, \quad a_6 > 0.$$

From the non-zero pattern and Lemma B.8 it follows that there do not exist $b, c \in S_+^9$ of order at least 2 such that $a = \mathrm{circ}(b)c$.

4. Primes in the doubly stochastic matrices

4.1. First characterization of a prime in the doubly stochastic matrices

Theorem 4.1. *(a) The matrix $A \in \mathrm{DS}_+^{n\times n}$ with $n \geqslant 2$ is a prime in the doubly stochastic matrices iff it is permutation equivalent to the direct sum of a fully indecomposable prime in the doubly stochastic matrices and an identity matrix, or, equivalently,*

$$A = P_1 \begin{pmatrix} A_1 & 0 \\ 0 & I \end{pmatrix} P_2 = P_1 (A_1 \oplus I) P_2 \tag{14}$$

with $P_1, P_2 \in P^{n\times n}$, $n_1, n_2 \in \mathbb{N}$, $n_1 \geqslant 2$, $n_1 + n_2 = n$, $A_1 \in \mathrm{DS}_+^{n_1\times n_1}$ a fully indecomposable prime in the doubly stochastic matrices, and $I \in \mathbb{R}_+^{n_2\times n_2}$.

(b) If

$$A = P_1 \begin{pmatrix} A_1 & 0 \\ 0 & I \end{pmatrix} P_2 = P_3 \begin{pmatrix} A_2 & 0 \\ 0 & I \end{pmatrix} P_4$$

with $A_1 \in \mathrm{DS}_+^{n_1\times n_1}$ and $A_2 \in \mathrm{DS}_+^{n_3\times n_3}$ are two factorizations as defined in (14) then $n_1 = n_3$ and $A_1 = P_5 A_2 P_6$ for $P_5, P_6 \in P^{n_1\times n_1}$.

The proof is analogous to that of Theorem 5.1 and omitted.

As argued in Section 2.3 the partial classification of primes in the doubly stochastic matrices has been reduced to solvability of equations. The solutions to these equations are described in Appendix C. In the next section examples of primes in the doubly stochastic matrices are described.

4.2. Examples of primes in the doubly stochastic matrices

Theorem 4.2. *Consider a doubly stochastic matrix $A \in \mathrm{DS}_+^{n\times n}$ with the convex sum representation $A = \sum_{i=1}^{n!} a_i P_i$ in which $n \geqslant 3$ and $a \in S_+^{n!}$ is of order 2. This matrix is a fully indecomposable prime in the doubly stochastic matrices iff there exists an $s \in (0,1)$ such that the matrix is permutation equivalent to*

$$sI + (1-s)W_n = \begin{pmatrix} s & 0 & \dots & 0 & 1-s \\ 1-s & s & & 0 & 0 \\ \vdots & & \ddots & & \vdots \\ 0 & 0 & & s & 0 \\ 0 & 0 & \dots & 1-s & s \end{pmatrix} \in \mathrm{DS}_+^{n\times n}. \tag{15}$$

Note that each element of the family of primes of Theorem 4.2 is a doubly stochastic circulant. However, not all primes in the doubly stochastic matrices are circulants, see Theorem 4.3.

Proof. ($\Rightarrow$) Let $A = \sum a_i P_i \in \mathrm{DS}_+^{n\times n}$ be a prime in the doubly stochastic matrices with $a \in S^{n!}$ of order 2. By premultiplication by a permutation matrix transform A to the form $a_1 I + a_j P_j$ for some $j \in \mathbb{Z}_n$. From Lemma C.1.b follows that there do not exist $b, c \in S_+^{n!}$ both of order at least 2 such that $a = L_m(b)c$.

From Theorem 4.1 follows that A is permutation equivalent to a matrix of the form $A_1 \oplus I$. By assumption the identity part cannot be present because A is fully indecomposable. From [5], Section 4.2, follows that $a_1 I + a_j P_j$ is fully indecomposable iff P_j is irreducible. P_j is irreducible iff it is cogredient to the shift or there exists a $Q \in P^{n\times n}$ such that $QP_jQ^{\mathrm{T}} = W_n$. Hence A is permutation equivalent to $a_1 I + a_j W_n$.

($\Leftarrow$) Let $A = sI + (1-s)W_n = \sum_{i=1}^{n!} a + iP_i$. From Proposition C.13 and $W_n = W_n^{\mathrm{T}}$ follows that there do not exist $b, c \in S_+^{n!}$ both of order at least 2 such that $a = L_m(b)c$. The map $(a_1 I + a_2 W_n) \mapsto a \in S_+^n$ is a bijection. From Lemma C.1 follows that A is a prime in the doubly stochastic matrices. □

Theorem 4.3. *Consider the family of doubly stochastic matrices*

$$A = \sum_{i=1}^{6} a_i P_i \in \mathrm{DS}_+^{3\times 3}, \tag{16}$$

in which $\{P_i, i \in \mathbb{Z}_6\}$ *is as defined in Example A.4 and* $a \in S_+^6$ *is of order 3. Then A is a fully indecomposable prime in the doubly stochastic matrices iff A is permutation equivalent to*

$$\sum_{i=1}^{6} a_i P_i = a_1 I + a_2 P_2 + a_5 P_5 = \begin{pmatrix} a_1 & 0 & a_2 + a_5 \\ a_2 & a_1 + a_5 & 0 \\ a_5 & a_2 & a_1 \end{pmatrix} \in \mathrm{DS}_+^{3\times 3}. \tag{17}$$

in which $a \in S_+^6$ *satisfies* $i(a) = (1, 2, 5) \subset \mathbb{Z}_6$.

Proof. ($\Rightarrow$) Let $A = \sum_{i=1}^{6} a_i P_i \in \mathrm{DS}_+^{3\times 3}$ be a prime in the doubly stochastic matrices. From Lemma C.1.(b) follows that there do not exist $b, c \in S_+^6$ both of

order at least 2 such that $a = L_m(b)c$. From Proposition C.14 then follows that the ordered triple $i(a) \subset \mathbb{Z}_6$ is different from $(1,2,3)$ and $(4,5,6)$. Any matrix $\sum_{i=1}^{6} a_i P_i$ with $i(a)$ one of the cases mentioned is permutation equivalent to the matrix of the statement of the theorem, which corresponds to $i(a) = (1,2,5)$. This can be proved because for any of the matrices A with $i(a)$ one of the cases mentioned the matrix has one column with no zero and two columns with one zero. By pre and post-multiplication by a permutation the matrix of any of the cases can be transformed to the form given in the theorem.

($\Leftarrow$) Note that $a \in S_+^6$ is of order 3 with $i(a) = (1,2,5)$. For the matrix $A = a_1 I + a_2 P_2 + a_5 P_5$ the map of A to $a \in S_+^6$ is a bijection. From Proposition C.14 follows that there do not exist $b, c \in S_+^6$ both of order at least 2 such that $a = L_m(b)c$. From Lemma C.1. (a) follows that A is a prime in the doubly stochastic matrices. □

The procedure described in Section 2.3 to determine whether or not a given matrix is a prime in the doubly stochastic matrices can then be followed for other matrices than the cases discussed above. The doubly stochastic matrices of the form $A = \sum a_i P_i \in \mathrm{DS}_+^{3\times 3}$ in which $a \in S_1^6$ with order $n(a) \geqslant 4$ have only partly been analyzed on whether they contain primes. It is conjectured that they do not. For the case in which $A = \sum a_i P_i \in \mathrm{DS}_+^{n\times n}$ with $n(a) = 3$ the solvability of the index equation is characterized by Lemma C.9. The solvability of the corresponding induced latin square is not yet characterized.

5. Primes in the positive matrices

5.1. First characterization of primes in the positive matrices

Theorem 5.1. *(a) The matrix $A \in \mathbb{R}_+^{n\times n}$ is a prime in the set of positive matrices iff it is monomially equivalent to the direct sum of a fully indecomposable doubly stochastic matrix that is a prime in the positive matrices and an identity matrix, or, equivalently, iff*

$$A = M_1 \begin{pmatrix} S & 0 \\ 0 & I \end{pmatrix} M_2 = M_1 (S \oplus I) M_2 \tag{18}$$

with $M_1, M_2 \in M_+^{n\times n}$, $n_1, n_2 \in \mathbb{N}$, $n_1 \geqslant 2$, $n_1 + n_2 = n$, $S \in \mathrm{DS}_+^{n_1 \times n_1}$ a fully indecomposable doubly stochastic matrix that is a prime in the positive matrices, and $I \in R_+^{n_2 \times n_2}$ the identity matrix.

(b) If

$$A = M_1 \begin{pmatrix} S_1 & 0 \\ 0 & I_{n_2} \end{pmatrix} M_2 = M_3 \begin{pmatrix} S_2 & 0 \\ 0 & I_{n_4} \end{pmatrix} M_4 \tag{19}$$

are two factorizations as in Eq. (18) with $S_1 \in \mathrm{DS}_+^{n_1 \times n_1}$ *and* $S_2 \in \mathrm{DS}_+^{n_3 \times n_3}$, *then* $n_1 = n_3$ *and*

$$S_1 = P_1 S_2 P_2 \tag{20}$$

for $P_1, P_2 \in P^{n_1 \times n_1}$.

Proof (a). ($\Rightarrow$) Let $A \in \mathbb{R}_+^{n \times n}$ be a prime in the positive matrices. Construct permutation matrices $P_1, P_2 \in P^{n \times n}$ such that

$$A = P_1 \begin{pmatrix} A_1 & 0 \\ 0 & D \end{pmatrix} P_2, \tag{21}$$

in which $n_1, n_2 \in \mathbb{N}$, $n_1 + n_2 = n$, $A_1 \in \mathbb{R}_+^{n_1 \times n_1}$ is an indecomposable matrix and $D \in \mathbb{R}_+^{n_2 \times n_2}$ is a strictly positive diagonal matrix. This step follows from [2], Section 3.4.23.

Determine strictly positive diagonal matrices $D_1, D_2 \in D_+^{n_1 \times n_1}$ such that $A_1 = D_1 S D_2$ for a doubly stochastic matrix $S \in \mathrm{DS}_+^{n_1 \times n_1}$. The existence of D_1, D_2 and S follows from the fact that A_1 is indecomposable and [4], Theorem. 6.2. See [19] for numerical algorithms.

Set

$$M_1 = P_1 \begin{pmatrix} D_1 & 0 \\ 0 & D \end{pmatrix}, \qquad M_2 = \begin{pmatrix} D_2 & 0 \\ 0 & I \end{pmatrix} P_2.$$

Eq. (18) holds in which $M_1, M_2 \in M_+^{n \times n}$ are monomial matrices and $S \in \mathrm{DS}_+^{n_1 \times n_1}$ is fully indecomposable, doubly stochastic, and a prime in the positive matrices.

Because A_1 is fully indecomposable and $D_1, D_2 \in D_+^{n_1 \times n_1}$ are strictly positive, one concludes that $S \in \mathrm{DS}_+^{n_1 \times n_1}$ is fully indecomposable. The matrix S fully indecomposable implies that $n_1 \geqslant 2$ and S is not a monomial.

It remains to show that S is a prime in the positive matrices. Suppose S is not a prime. Since S is not a monomial, it follows that there exists a factorization $S = BC$ with neither B nor C a monomial. Then

$$A = B_1 C_1, \quad B_1 = M_1 \begin{pmatrix} B & 0 \\ 0 & I \end{pmatrix}, \quad C_1 = \begin{pmatrix} C & 0 \\ 0 & I \end{pmatrix} M_2$$

is a factorization of A with neither B_1 nor C_1 a monomial. This contradicts the assumption that A is a prime.

($\Leftarrow$) It follows from the fact that S is a prime in the positive matrices and [2], Section 3.4.24, that $(S \oplus I)$ is a prime in the positive matrices. Hence $A = M_1(S \oplus I)M_2$ is prime in the positive matrices. (b) The proof of this part is omitted to save space. In the proof use may be made of the uniqueness of the transformation to doubly stochastic form, see [4], Theorem 6.2. □

Theorem 5.1 reduces the classification of primes in the positive matrices to the classification of fully indecomposable doubly stochastic matrices which are primes in the positive matrices.

A prime in the positive matrices that is also doubly stochastic is a prime in the doubly stochastic matrices. Theorem 4.3 establishes the existence of a doubly stochastic matrix that is a prime in the doubly stochastic matrices but that is not a prime in the positive matrices. That it is not a prime in the positive matrices follows from [2], Corollary 3.4.20. The classification of fully indecomposable doubly stochastic matrices that are primes in the positive matrices is only partly solved.

5.2. *Examples of primes in the positive matrices*

Proposition 5.2. *Consider the matrix*

$$A = \sum_{i=1}^{n!} a_i P_i \in \mathbb{R}_+^{n\times n}, \tag{22}$$

in which $n \geqslant 3$, $\{P_i, i \in Z_{n!}\}$ *is an enumeration of the permutations in* $P^{n\times n}$, *and* $a \in R_+^{n!}$ *is of order 2. This matrix is a fully indecomposable prime in the positive matrices iff there exists an* $s \in (0,1)$ *such that the matrix is monomially equivalent to the matrix*

$$sI + (1-s)W_n = \begin{pmatrix} s & 0 & \dots & 0 & 1-s \\ 1-s & s\dots & 0 & 0 & \\ \vdots & \vdots & \ddots & & \vdots \\ 0 & 0 & & s & 0 \\ 0 & 0 & \dots & 1-s & s \end{pmatrix}. \tag{23}$$

Proof. ($\Leftarrow$) That (23) is a prime in the positive matrices follows from [2], Theorem 2.6. That this matrix is fully indecomposable follows from [5], Section 4.2.

($\Rightarrow$) Note that

$$B = \frac{1}{\sum_{i=1}^{n!} a_i} \sum a_i P_i \in \mathrm{DS}_+^{n\times n}$$

and that B is monomially equivalent to A. Then B is a prime in the doubly stochastic matrices. From Theorem 4.2 follows that B is permutation equivalent to the matrix displayed in (23). Hence A is monomially equivalent to the matrix displayed in (23). □

6. Concluding remarks

Results have been presented on the classification of primes in the doubly stochastic circulants, the doubly stochastic matrices, and the positive matrices. Primes in several subclasses of the classes mentioned have been characterized. The general classification is far from being solved.

What needs to be investigated to solve completely the classification problems? The classification problem of primes in the doubly stochastic circulants has been reduced to the solution of an equation over a doubly stochastic circulant. The cases of this equation that have been solved point to discrete and to analytic conditions for the existence of a solution. The conditions vary with the discrete parameters of the problem. It is not clear whether general solvability conditions can be formulated.

The classification of primes in the doubly stochastic matrices has been reduced to solvability of an equation over a doubly stochastic latin square. Conditions for the existence of a solution of the latter equation have been derived in two cases. A general result will probably have to be formulated in both discrete and analytic conditions.

The classification of primes in the positive matrices may be based on the classification of fully indecomposable doubly stochastic matrices that are primes in the doubly stochastic matrices. Here much research remains to be done.

Appendix A. Matrix preliminaries

A.1. Latin squares

Definition A.1. A subset $PC = \{P_i,\ i \in I\} \subset P^{n\times n}$ is said to be a *permutation covering* of $\mathbb{R}_+^{n\times n}$ if

$$\sum_{i\in I} P_i = E_n,$$

where $E_n \in \mathbb{R}_+^{n\times n}$ is such that $[(E_n)_{ij}] = 1$ for all $i, j \in \mathbb{Z}_n$.

A permutation covering consists of exactly n permutations. Which subsets of $P^{n\times n}$ form a permutation covering? The set of multiple shifts

$$\{W_n^0, W_n^1, \ldots, W_n^{n-1}\} \subset P^{n\times n}$$

is a permutation covering of $\mathbb{R}_+^{n\times n}$.

A latin square is a well known concept, see [8]. Another definition is presented below that seems more suitable for this paper than one of the definitions of the literature.

Definition A.2. A matrix $A \in \mathbb{R}_+^{n\times n}$ will be called a *positive latin square* if there exists a permutation covering $\{P_i, i \in I\} \subset P^{n\times n}$ of $\mathbb{R}_+^{n\times n}$ and a vector $a \in \mathbb{R}_+^n$ such that

$$A = \sum_{i=1}^{n} a_i P_i. \tag{A.1}$$

In this case define the map $L : \mathbb{R}_+^n \to \mathbb{R}_+^{n\times n}$ by $A = L(a) = \sum a_i P_i$. The matrix $A \in \mathbb{R}_+^{n\times n}$ is called a *doubly stochastic latin square* if it is a positive latin square and doubly stochastic. In this case it admits a representation as the matrix displayed in (A.1) with $a \in S_+^n$.

An example of a positive latin square is a circulant $\mathrm{circ}(a) \in \mathbb{R}_+^{n\times n}$ with $a \in \mathbb{R}_+^n$. If in addition $a \in S_+^n$ then $\mathrm{circ}(a) \in \mathrm{DS}_+^{n\times n}$. It follows from the definition of a positive latin square, in particular from a permutation covering, that every row and every column of such a matrix $A = \sum a_i P_i$ is a permutation of the elements of the vector $a \in \mathbb{R}_+^n$. A characterization of the set of latin squares follows from a characterization of the set of permutation coverings.

Definition A.3. The *latin square induced by multiplication of permutation* in $P^{n\times n}$ is defined as

$$L_m : \mathbb{R}_+^{n!} \to \mathbb{R}_+^{n!\times n!}, \quad [L_m(x)_{kj}] = x_i, \quad \text{if} \quad P_i P_j = P_k, \tag{A.2}$$

where P_i, P_j, P_k are elements of an enumeration of $P^{n\times n}$.

It can be shown that a latin square induced by multiplication as defined in Definition A.3 is a latin square as defined in Definition A.2.

Example A.4. Consider the following enumeration of the elements of $P^{3\times 3} = \{P_1, \ldots, P_6\}$:

$$P_1 = I, \quad P_2 = W_3 = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, \quad P_3 = W_3^2 = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}, \tag{A.3}$$

$$P_4 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}, \quad P_5 = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}, \quad P_6 = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}. \tag{A.4}$$

The latin square in $\mathbb{R}^{3!\times 3!}$ induced by multiplication of permutations in $P^{3\times 3}$ is given by

$$L_m(x) = \begin{pmatrix} x_1 & x_3 & x_2 & x_4 & x_5 & x_6 \\ x_2 & x_1 & x_3 & x_6 & x_4 & x_5 \\ x_3 & x_2 & x_1 & x_5 & x_6 & x_4 \\ x_4 & x_6 & x_5 & x_1 & x_2 & x_3 \\ x_5 & x_4 & x_6 & x_3 & x_1 & x_2 \\ x_6 & x_5 & x_4 & x_2 & x_3 & x_1 \end{pmatrix} = \sum_{i=1}^{6} x_i P_i. \tag{A.5}$$

A.2. Doubly stochastic matrices

The set of doubly stochastic matrices in $\mathrm{DS}_+^{n\times n}$ is a convex polyhedron of dimension $(n-1)^2$ whose extremal elements are the set of permutation matrices according to a theorem of Birkhoff [2], Section 2.5.6. A matrix $A \in \mathbb{R}_+^{n\times n}$ is said to have a representation as a *convex sum of permutations* if

$$A = \sum_{i=1}^{n!} x_i P_i, \tag{A.6}$$

where $x \in S_+^{n!}$ and $\{P_i, i \in \mathbb{Z}_{n!}\} = P^{n\times n}$ is the set of permutations of size $n \times n$. Such a matrix is said to be nontrivial if it is not itself a permutation, or, equivalently, if the vector x is of order 2 or larger. Note that a circulant and a positive latin square in $\mathbb{R}_+^{n\times n}$ have representations as convex sums of permutations in which the sum is over n permutations only and in the case of a doubly stochastic circulant the permutations are the shifts. Given a matrix $A \in \mathrm{DS}_+^{n\times n}$, its representation as a convex sum of permutations as in Eq. (A.6) is not unique.

Notation and a result on the specialization order are stated below. Sources on this are [17], Ch. V and [16]. For $x \in \mathbb{R}_+^n$ let

$$x_{\downarrow} = \begin{pmatrix} x_{[1]} \\ \vdots \\ x_{[n]} \end{pmatrix} \in \mathbb{R}_+^n, \quad x_{[1]} \geqslant x_{[2]} \geqslant \cdots \geqslant x_{[n]} \tag{A.7}$$

denote the vector with the components of x in decreasing order. For $x, y \in R_+^n$ one says that x is *majorized* by y or that y *majorizes* x, if

$$\sum_{i=1}^{k} x_{[i]} \leqslant \sum_{i=1}^{k} y_{[i]}, \quad k = 1, 2, \ldots, n-1, \qquad \sum_{i=1}^{n} x_{[i]} = \sum_{i=1}^{n} y_{[i]}. \tag{A.8}$$

Denote by $x \preceq y$ that x is majorized by y and call $\preceq$ the *specialization order* on $\mathbb{R}_+^n$. It follows from [16], Section X, that, with $x, y \in \mathbb{R}_+^n$, $x \preceq y$ iff there exists a $S \in \mathrm{DS}_+^{n\times n}$ such that $x = Sy$.

Proposition A.5. *Let $a, b, c \in S_+^n$ and $L : S_+^n \to \mathbb{R}_+^{n\times n}$ be the map of a doubly stochastic latin square. Assume that $a = L(b)c$ holds. If $a \in S_+^n$ is a vector of*

order $n(a) \in \mathbb{N}_n$ *then both* b *and* c *are vectors of orders at most* $n(a)$, *or* $n(b) \leqslant n(a)$ *and* $n(c) \leqslant n(a)$.

Note that the result of the above proposition also holds if $a = \mathrm{circ}(b)c$.

Proof. The assumptions that $b \in S_+^n$ and L is a latin square imply that $L(b) \in \mathrm{DS}_+^{n\times n}$. It then follows from the characterization of the specialization order and $a = L(b)c$ that $a \preceq c$, or, equivalently, that

$$\sum_{i=1}^{k} a_{[i]} \leqslant \sum_{i=1}^{k} c_{[i]}, \quad k = 1, 2, \ldots, n-1, \qquad \sum_{i=1}^{n} a_{[i]} = \sum_{i=1}^{n} c_{[i]} = 1.$$

If a is a vector of order m then

$$1 = \sum_{i=1}^{m} a_{[i]} \leqslant \sum_{i=1}^{m} c_{[i]}$$

and hence, because $c \in S_+^n$, $\sum_{i=1}^{m} c_{[i]} = 1$. Thus c is a vector of order at most m. Because $a = L(b)c$ there also holds $a = L_1(c)b$ for another positive latin square L_1. The result for c then follows by symmetry. □

Appendix B. Proofs for primes in the doubly stochastic circulants

B.1. Polynomial representation of doubly stochastic circulants

Any $n \times n$ circulant matrix A has a *unique* representation as a polynomial of degree $n-1$ in the shift operator W_n, $A = \sum_{i=0}^{n-1} a_i W_n^i$. The polynomial map associated to A, $a(z) = \sum_{i=0}^{n-1} a_i z^i$, is called its *representer* or *incidence polynomial*. It is a *ring homomorphism*, [6], p. 68–70. Since $W_n^n = I$, in all operations involving representers of $n \times n$ circulant matrices, the nth power z^n must be treated as 1, i.e., the polynomial $z^n - 1$ is equivalent to the zero polynomial. The homomorphism above becomes a ring isomorphism if the ring of polynomials is substituted by the quotient ring $\mathbb{R}[z]/(z^n - 1)$.

From these general facts it follows in particular that the representer of a doubly stochastic circulant $A \in \mathrm{DSC}_+^{n\times n}$ is a polynomial in z with positive coefficients summing up to one, i.e., with the property $a(1) = 1$. The semi-ring of polynomials with positive coefficients will be denoted by $\mathbb{R}_+[z]$, the semi-ring of polynomials $p(z)$ with positive coefficients normalized such that $p(1) = 1$ by $S_+[z]$, and the quotient semi-ring of $\mathbb{R}_+[z]$ ($S_+[z]$, respectively) modulo $z^n - 1$ by $\mathbb{R}_+[z]/(z^n - 1)$ ($S_+[z]/(z^n - 1)$, respectively). Clearly $\mathrm{DSC}_+^{n\times n}$ and

$S_+[z]/(z^n-1)$ are isomorphic as semi-rings. A matrix $A \in \mathrm{DSC}_+^{n\times n}$ is a unit if and only if its representer $a(z)$ is a monomial in $S_+[z]/(z^n-1)$, i.e., $a(z)=z^k$.

Definition B.1. A *prime* in the quotient semi-ring $S_+[z]/(z^n-1)$ is a polynomial $a(z) \in S_+[z]/(z^n-1)$ such that
1. $a(z)$ is not a monomial, i.e., $a(z) \neq z^k$;
2. if $a(z)=b(z)c(z)$ with $b(z),c(z) \in S_+[z]/(z^n-1)$, then either $b(z)$ or $c(z)$ is a monomial.

Whenever $a(z)=b(z)c(z)$ with $b(z),c(z) \in S_+[z]/(z^n-1)$, neither of them being monomial, $b(z)$ (or $c(z)$) is said to *divide* $a(z)$ *strongly*.

It is obvious that for a positive factorization $a(z)=b(z)c(z)$, $a(z) \in S_+[z]/(z^n-1)$, the factors $b(z),c(z) \in \mathbb{R}_+[z]/(z^n-1)$ can both be normalized by dividing them by positive numbers $b(1),c(1)$ such that $a(1)=1=b(1)c(1)$. Therefore, taking as group of units the set $\{\alpha z^k \mid \alpha \in \mathbb{R}_+,\ k \in \mathbb{N}\}$, primes in $\mathbb{R}_+[z]/(z^n-1)$ are essentially the same as primes in $S_+[z]/(z^n-1)$, up to multiplication with a constant.

Proposition B.2. *A matrix $A \in \mathrm{DSC}_+^{n\times n}$ is a prime in the doubly stochastic circulants if and only if its representer is a prime in the quotient semi-ring $S_+[z]/(z^n-1)$.*

Proof. Let

$$A=\sum_{i=0}^{n-1} a_i W_n^i, \qquad a(z)=\sum_{i=0}^{n-1} a_i z^i.$$

A is a prime in the doubly stochastic circulants if and only if
1. A is not a monomial;
2. if $A=BC$ with $B,C \in \mathrm{DSC}_+^{n\times n}$, then either B or C is a monomial.

Condition 1 is equivalent to $a(z)$ not being a monomial. Let $B=\sum b_i W_n^i$ and $C=\sum c_i W_n^i$. Their representers are $b(z)=\sum b_i z^i$ and $c(z)=\sum c_i z^i$, respectively. It follows that Condition 2 is equivalent to '*if* $a(z)=b(z)c(z)$ *with* $b(z),c(z) \in S_+[z]/(z^n-1)$, *then either* $b(z)$ *or* $c(z)$ *is a monomial*'. So A is a prime in the doubly stochastic circulants if and only if $a(z)$ is a prime in the quotient semi-ring $S_+[z]/(z^n-1)$. □

The following example shows that prime in $\mathbb{R}_+[z]/(z^n-1)$ is not the same as prime in $\mathbb{R}_+[z]$.

Example B.3. Consider the polynomial $f(z)=z^3+z+10$. This polynomial can be factorized as $f(z)=(z+2)(z^2-2z+5)=(z+2)(z-1+2i)(z-1-2i)$. None of the factors of $f(z)$ in $\mathbb{R}_+[z]$ is monomial, so $f(z)$ is prime in $\mathbb{R}_+[z]$. But in $\mathbb{R}_+[z]/(z^4-1)$, $f(z)=(z^3+\lambda z^2)(z^2+\mu z)$ with $\lambda=5+2\sqrt{6}>0$ and

$\mu = 5 - 2\sqrt{6} = 5 - \sqrt{24} > 0$. So $f(z)$ is not prime in $\mathbb{R}_+[z]/(z^4 - 1)$. It follows that $f(z)/12$ is not prime in $S_+[z]/(z^4 - 1)$ and hence

$$A = \frac{1}{12}\begin{pmatrix} 10 & 1 & 0 & 1 \\ 1 & 10 & 1 & 0 \\ 0 & 1 & 10 & 1 \\ 10 & 1 & 1 & 0 \end{pmatrix}$$

is not prime in $\mathrm{DSC}_+^{4\times 4}$.

The problem is to find a factorization in $\mathbb{R}_+[z]/(z^n - 1)$ of a polynomial $a(z) \in \mathbb{R}_+[z]/(z^n - 1)$.

Lemma B.4. *Consider $a(z) \in \mathbb{R}_+[z]/(z^n - 1)$. There exist polynomials $b(z), c(z) \in \mathbb{R}_+[z]/(z^n - 1)$, neither of which is a monomial, such that*

$$a(z) = b(z)c(z) \pmod{z^n - 1}$$

if and only if there exists a polynomial $g(z) \in \mathbb{R}_+[z]$ of degree strictly less than $n - 1$, such that

$$a(z) + (z^n - 1)g(z) \in \mathbb{R}_+[z]$$

can be factorized into $h(z)k(z)$ in $\mathbb{R}_+[z]$ with neither $h(z) \pmod{z^n - 1}$ nor $k(z) \pmod{z^n - 1}$ monomial.

A conclusion of Lemma B.4 is that the determination of primes in $\mathbb{R}_+[z]/(z^n - 1)$ by a transformation of the factorization in $\mathbb{R}_+[z]/(z^n - 1)$ to one in $\mathbb{R}_-[z]$ is not so practical. Note that the factorization in $\mathbb{R}_+[z]$ must be carried out for $a(z) + g(z)(z^n - 1)$ for all $g \in \mathbb{R}_-[z]$ of degree less than $n - 1$.

Proof. ($\Rightarrow$) Assume there exist polynomials $b(z), c(z) \in \mathbb{R}_+[z]/(z^n - 1)$, neither of which is a monomial, such that $a(z) = b(z)c(z) \pmod{z^n - 1}$. This is equivalent to $a(z) + (z^n - 1)g(z) = b(z)c(z)$ for a polynomial $g(z) \in \mathbb{R}[z]$. Since $b(z), c(z) \in \mathbb{R}_+[z]/(z^n - 1)$, their degrees are less than or equal to $n - 1$, so $\deg((z^n - 1)g(z)) \leqslant \deg(b(z)c(z)) \leqslant 2n - 2$, i.e., $\deg(g(z)) \leqslant n - 2$. Let $g(z) = g_0 + g_1 z + \cdots + g_{n-2}z^{n-2}$, for $g_i \in \mathbb{R}$. Then $b(z)c(z) = a(z) - g(z) + g_0 z^n + g_1 z^{n+1} + \cdots + g_{n-2}z^{2n-2}$. Now $g_i \geqslant 0$, since $\deg(a(z) - g(z)) \leqslant n - 1$ and $b(z)c(z) \in \mathbb{R}_+[z]$. It follows that $g(z) \in \mathbb{R}_+[z]$ and $a(z) + (z^n - 1)g(z)$ can be factorized into $b(z)c(z)$ with $b(z) \pmod{z^n - 1}$ and $c(z) \pmod{z^n - 1}$ not monomials.

($\Leftarrow$) Assume there exists a polynomial $g(z) \in \mathbb{R}_-[z]$ of degree strictly less than $n - 1$, such that for

$$f(z) = a(z) + (z^n - 1)g(z) \in \mathbb{R}_+[z]$$

there exist polynomials $h(z), k(z) \in \mathbb{R}_+[z]$, such that $f(z) = h(z)k(z)$. Let $b(z) = h(z) \pmod{z^n - 1}$ and $c(z) = k(z) \pmod{z^n - 1}$. Then

$$\begin{aligned} a(z) &= f(z) \pmod{z^n - 1} = h(z)k(z) \pmod{z^n - 1} \\ &= b(z)c(z) \pmod{z^n - 1}. \end{aligned}$$

From the assumptions it follows that $b(z)$ and $c(z)$ are not monomials. □

The following proposition is a general result on the classification of primes in $S_+[z]/(z^n - 1)$, or equivalently, the classification of primes in the doubly stochastic circulants.

Proposition B.5. *The polynomial*

$$p(z) = \sum_{i=0}^{n-1} p_i z^i \in \mathbb{R}_+[z]/(z^n - 1), \tag{B.1}$$

with $p_i > 0$ for all $i \in \mathbb{N}_{n-1}$, is not prime in the quotient semi-ring $\mathbb{R}_+[z]/(z^n - 1)$.

Proof. Consider first the polynomial $p(z)$ with $p_i = p_j = \bar{p}$ for all $i, j \in \mathbb{N}_{n-1}$. Then

$$\begin{aligned} p(z) &= \sum_{i=0}^{n-1} p_i z^i = \sum_{i=0}^{n-1} \bar{p} z^i = \frac{1}{2}(z+1)\sum_{i=0}^{n-1} \bar{p} z^i \\ &= \frac{1}{2}(z+1)p(z) \pmod{z^n - 1}. \end{aligned}$$

So $p(z)$ is not prime in the quotient semi-ring $\mathbb{R}_+[z]/(z^n - 1)$. Otherwise, if there exist $i, j \in \mathbb{N}_{n-1}$ such that $p_i \neq p_j$, choose

$$0 < a < \min\left\{ \frac{p_0}{p_{n-1}}, \frac{p_i}{p_{i-1}},\ i \in \mathbb{Z}_{n-1} \right\}.$$

Since $p_i > 0$ for all $i \in \mathbb{N}_{n-1}$, the minimum mentioned above is strictly positive, so such an a exists. The claim is that $a < 1$. Indeed, suppose $a \geqslant 1$. Then $p_0/p_{n-1} > a \geqslant 1$ and $p_i/p_{i-1} > a \geqslant 1$ for all $i \in \mathbb{Z}_{n-1}$, so

$$1 \leqslant a^{n-1} < \frac{p_0}{p_{n-1}} \prod_{i=1}^{n-1} \frac{p_i}{p_{i-1}} = 1.$$

This is a contradiction, so $a < 1$. Now $p(z)$ can be factorized in $b(z)c(z)$ in $\mathbb{R}_+[z]/(z^n - 1)$ with

$$b(z) = \frac{1}{1 - a^n} \sum_{i=0}^{n-1} a^i z^i, \qquad c(z) = p_0 - a p_{n-1} + \sum_{i=1}^{n-1} (p_i - a p_{i-1}) z^i.$$

Indeed,

$$b(z)c(z) = \sum_{i=0}^{n-1} b_i z^i \sum_{j=0}^{n-1} c_j z^j$$
$$= \sum_{k=0}^{n-1} \left(\sum_{i=0}^{n-1} b_{k-i|n} c_i \right) z^k \pmod{z^n - 1},$$

and since for all $k \in \mathbb{N}_{n-1}$

$$\sum_{i=0}^{n-1} b_{k-i|n} c_i = \sum_{i=0}^{k} b_{k-i} c_i + \sum_{i=k+1}^{n-1} b_{n+k-i} c_i$$
$$= \frac{1}{1-a^n} \left\{ a^k (p_0 - a p_{n-1}) + \sum_{i=1}^{k} a^{k-i} (p_i - a p_{i-1}) \right.$$
$$\left. + \sum_{i=k+1}^{n-1} a^{n+k-i} (p_i - a p_{i-1}) \right\}$$
$$= \frac{1}{1-a^n} \left(a^k p_0 - a^{k+1} p_{n-1} + a^{k-1} p_1 - a^k p_0 + \ldots + a^0 p_k \right.$$
$$\left. - a p_{k-1} + a^{n-1} p_{k+1} - a^n p_k + \cdots + a^{k+1} p_{n-1} - a^{k+2} p_{n-2} \right)$$
$$= \frac{1}{1-a^n} (1 - a^n) p_k = p_k,$$

it follows that $p(z) = b(z)c(z) \pmod{z^n - 1}$. Because $a < 1$, for $i \in \mathbb{N}_{n-1}$ $b_i = a^i/(1-a^n) > 0$, and since $a < p_0/p_{n-1}$ and $a < p_i/p_{i-1}$ for $i \in \mathbb{Z}_{n-1}$, also $c_0 = p_0 - a p_{n-1} > 0$ and for $i \in \mathbb{Z}_{n-1}$ $c_i = p_i - a p_{i-1} > 0$. So $b(z)$ and $c(z)$ in $\mathbb{R}_+[z]/(z^n - 1)$ are not monomials, from which it follows that $p(z)$ is not a prime in the quotient semi-ring $\mathbb{R}_+[z]/(z^n - 1)$. □

B.2. Reduction of classification problem

Below it will be shown that the classification of a prime in the doubly stochastic circulants is equivalent to the solvability of a linear equation over a doubly stochastic circulant. The latter problem is analyzed in Section B.3.

Lemma B.6 *Assume $A \in \mathrm{DSC}_+^{n\times n}$ is of order larger or equal than 2, say with representation $A = \sum a_i P_i$. Then the following statements are equivalent.*

a. The matrix $A \in \mathrm{DSC}_+^{n\times n}$ is a prime in the doubly stochastic circulants.

b. There do not exist $b, c \in S_+^n$ each of which is of order at least 2 such that $a = \mathrm{circ}(b)c$.

The proof of this result is omitted. It is analogous to that of Lemma C.1.

B.3. Linear equations over doubly stochastic circulants

Problem B.7. *Solvability of a linear equation over a doubly stochastic circulant.* Let $a \in S_+^n$ be a vector of order at least 2. Determine conditions on this vector such that there exist vectors $b, c \in S_+^n$, each of which is of order at least 2, such that

$$a = \mathrm{circ}(b)c. \tag{B.2}$$

Lemma B.8. *Let $a \in S_+^n$ be a vector with order $n(a) \geqslant 2$. If there exist $b, c \in S_+^n$ each of which is of order at least 2 such that Eq. (B.2) holds then*

$$i(a) = \bigcup_{j=1, c_j>0}^{n} i(W_n^{j-1}b).$$

The proof of this result is omitted. It is analogous to that of Lemma C.3.

Below solutions are presented to several special cases of Problem B.7. The results are ordered by the order of the vector $a \in S_+^n$. It follows from Proposition B.5 that only a matrix in $\mathrm{DSC}_+^{n\times n}$ of order smaller or equal than $n-1$ is eligible to be a prime.

Proposition B.9. *Let $n \in \mathbb{Z}_+$, $n \geqslant 3$, and $a \in S_+^n$ with order $n(a) = 2$. Then there do not exist $b, c \in S_+^n$ of order at least 2 such that $a = \mathrm{circ}(b)c$.*

Proof. Assume there exist $b, c \in S_+^n$ of order at least 2 such that $a = \mathrm{circ}(b)c$ holds. Then, Proposition A.5, $n(b) \leqslant n(a) = 2$ and $n(c) \leqslant n(a) = 2$, hence $n(b) = n(c) = 2$. From Lemma B.8 it follows that

$$i(a) = \bigcup_{j=1, c_j>0}^{n} i(W_n^{j-1}b), \tag{B.3}$$

while

$$2 = n(a) < 3 \leqslant n\left(\bigcup_{j=1, c_j>0}^{n} i(W_n^{j-1}b)\right), \tag{B.4}$$

where the last inequality follows because the union is exactly over two values of j, say j_1, j_2, with $n(W_n^{j_1-1}b) = 2$, $i(W_n^{j_1-1}b) \neq i(W_n^{j_2-1}b)$, and there may be overlap between $i(W_n^{j_1-1}b)$, $i(W_n^{j_2-1}b)$. The Eqs. (B.3) and (B.4) are incompatible. This establishes the contradiction. □

The above result is illustrated by the following two examples.

Example B.10. Let $a \in S_+^4$ and suppose there exist $b, c \in S_+^4$ of order 2 such that

$$\begin{pmatrix} a_1 \\ a_2 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} b_1 & 0 & 0 & b_2 \\ b_2 & b_1 & 0 & 0 \\ 0 & b_2 & b_1 & 0 \\ 0 & 0 & b_2 & b_1 \end{pmatrix} \begin{pmatrix} c_1 \\ c_2 \\ 0 \\ 0 \end{pmatrix}.$$

Then

$$\begin{aligned} i(a) &= \{1,2\}, \qquad \bigcup_{j=1, c_j>0}^{n} i(W_4^{j-1}b) = i(b) \cup i(W_4 b) \\ &= \{1,2\} \cup \{2,3\} = \{1,2,3\}. \end{aligned}$$

Hence such b, c cannot exist. The other possibilities for a, b, c similarly result in impossibilities.

Example B.11. Let $a \in S_+^4$ with order $n(a) = 3$ and suppose there exist $b, c \in S_+^4$ of order 2 such that

$$\begin{pmatrix} a_1 \\ a_2 \\ a_3 \\ 0 \end{pmatrix} = \begin{pmatrix} b_1 & 0 & 0 & b_2 \\ b_2 & b_1 & 0 & 0 \\ 0 & b_2 & b_1 & 0 \\ 0 & 0 & b_2 & b_1 \end{pmatrix} \begin{pmatrix} c_1 \\ c_2 \\ 0 \\ 0 \end{pmatrix} = \operatorname{circ}(b)c.$$

Then $i(a) = \{1,2,3\} =: \cup_{j=1, c_j>0}^{n} i(W_4^{j-1}b)$ hence the necessity condition of Lemma B.8 is satisfied. To determine whether a matrix

$$A = \sum_{i=1}^{n} a_i W_n^{i-1} \in \mathrm{DSC}_{-}^{n\times n}, \quad a \in S_+^n, \quad 2 < n(a) < n$$

is prime, it has to be proved that there do not exist $b, c \in S_+^n$ with $2 \leqslant n(b) \leqslant n(a)$ and $2 \leqslant n(c) \leqslant n(a)$ such that $a = \operatorname{circ}(b)c$. Examples on how to solve this problem follow below.

Proposition B.12. *Let $a \in S_+^3$ be of order 3. Then there exist $b, c \in (0,1)$ such that*

$$a = \begin{pmatrix} a_1 \\ a_2 \\ a_3 \end{pmatrix} = \begin{pmatrix} b & 0 \\ 1-b & b \\ 0 & 1-b \end{pmatrix} \begin{pmatrix} c \\ 1-c \end{pmatrix} \tag{B.5}$$

if and only if $a_2^2 \geqslant 4a_1a_3$.

Proof. Let $a \in S_+^3$ be of order 3. Then $a_2 = 1 - a_1 - a_3$. Note that (B.5) is equivalent to

$$a_1 = bc, \tag{B.6}$$

$$a_2 = (1-b)c + b(1-c), \tag{B.7}$$

$$a_3 = (1-b)(1-c). \tag{B.8}$$

It is claimed that (B.6)–(B.8) is equivalent to (B.6), (B.8). This is proven by showing that (B.6), (B.8) implies (B.7). Indeed, using (B.6) and (B.8),

$$(1-b)c + b(1-c) = c - bc + b - bc = 1 - bc - (1-b)(1-c) = 1 - a_1 - a_3 = a_2.$$

Consider the calculations

$$a_1 = bc, a_3 = (1-b)(1-c) = 1 - b - c + bc = 1 - (b+c) + a_1, b + c = 1 + a_1 - a_3.$$

Thus (B.6) and (B.8) are equivalent to $bc = a_1$ and $b + c = 1 + a_1 - a_3$. Consider the polynomial

$$(z+b)(z+c) = z^2 + (b+c)z + bc = z^2 + (1 + a_1 - a_3)z + a_1. \tag{B.9}$$

There exist $b, c \in \mathbb{R}$ if and only if $D := (1 + a_1 - a_3)^2 - 4a_1 \geqslant 0$. Now

$$D = (1 + a_1 - a_3)^2 - 4a_1 = (2a_1 + a_2)^2 - 4a_1 = 4a_1^2 + 4a_1a_2 + a_2^2 - 4a_1 = a_2^2 + 4a_1(a_1 + a_2 - 1) = a_2^2 - 4a_1a_3.$$

So if $b, c \in (0,1)$ exist, then $a_2^2 \geqslant 4a_1a_3$. Conversely, assume $a_2^2 \geqslant 4a_1a_3$. Then D defined above is nonnegative, so the roots of the polynomial (B.9) are real, i.e., there exist $b, c \in \mathbb{R}$ such that (B.6), (B.7), and (B.8) hold. The question is whether $b, c \in (0,1)$. Since $bc = a_1 > 0$ and $b + c = 1 + a_1 - a_3 = 2a_1 + a_2 > 0$, also $b > 0$ and $c > 0$. It follows from $bc = a_1 < 1$ that $b < 1$ or $c < 1$. If $b < 1$, then from (B.8) it follows that

$$1 - c = \frac{a_3}{1-b} > 0,$$

so $c < 1$. The same reasoning gives that if $c < 1$, then also $b < 1$. It follows that there exist $b, c \in (0,1)$ such that (B.6), (B.7), and (B.8) hold.

Example B.13. For the vector

$$a = \frac{1}{3}\begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} \in S_+^3$$

there do not exist $b, c \in (0,1)$ such that a can be written in the form (B.6). This follows because the inequality $a_2^2 \geqslant 4a_1a_3$ is equivalent to $(1/3)^2 \geqslant 4(1/3)^2$, which is false.

Proposition B.14. *Let $a \in S_+^4$ be of order 3. There exist $b, c \in S_+^4$ of order at least 2 such that*

$$a = \begin{pmatrix} a_1 \\ a_2 \\ a_3 \\ a_4 \end{pmatrix} = \operatorname{circ}(b)c$$

if and only if either $a_1^2 + a_3^2 \geqslant 4a_2a_4 > 0$ or $a_2^2 + a_4^2 \geqslant 4a_1a_3 > 0$.

Proof. Let $a \in S_+^4$ be of order 3. The possible patterns of the vector a are

$$a^{(0)} = \begin{pmatrix} a_1 \\ a_2 \\ a_3 \\ 0 \end{pmatrix}, \quad a^{(1)} = \begin{pmatrix} a_1 \\ a_2 \\ 0 \\ a_4 \end{pmatrix}, \quad a^{(2)} = \begin{pmatrix} a_1 \\ 0 \\ a_3 \\ a_4 \end{pmatrix}, \quad a^{(3)} = \begin{pmatrix} 0 \\ a_2 \\ a_3 \\ a_4 \end{pmatrix}.$$

Note that $a^{(i)} = W_4^{4-i}a^{(0)}$, so there exist $b, c \in S_+^4$ of order at least 2 such that $a^{(0)} = \operatorname{circ}(b)c$ if and only if $a^{(i)} = \operatorname{circ}(W_4^{4-i}b)c$. It will be proven that there exist $b, c \in S_+^4$ of order at least 2 such that

$$\begin{pmatrix} a_1 \\ a_2 \\ a_3 \\ 0 \end{pmatrix} = \operatorname{circ}(b)c$$

if and only if $a_2^2 + a_4^2 \geqslant 4a_1a_3 > 0$.

($\Rightarrow$) Consider $a^{(0)}$. Assume there exist $b, c \in S_+^4$ of order at least 2 such that $a^{(0)} = \operatorname{circ}(b)c$. From Proposition A.5 it follows that $n(b) \leqslant n(a) = 3$ and $n(c) \leqslant n(a) = 3$. The possible values of the pair $(n(b), n(c))$ are $(3,3), (3,2), (2,3), (2,2)$. The first three possibilities cannot occur as can be seen from the nonzero pattern of the vectors. There remains the case $(n(b), n(c)) = (2,2)$. The possible choices for nonzero patterns of c, $i(c)$, are $\{1,2\}, \{2,3\}, \{3,4\}$, and $\{1,4\}$. The patterns $\{1,3\}$ and $\{2,4\}$ are not possible, as can be seen from the nonzero pattern of b. It follows that the possible choices for b and c are

$$a^{(0)} = \begin{pmatrix} a_1 \\ a_2 \\ a_3 \\ 0 \end{pmatrix} = \begin{pmatrix} b_1 & 0 & 0 & 1-b_1 \\ 1-b_1 & b_1 & 0 & 0 \\ 0 & 1-b_1 & b_1 & 0 \\ 0 & 0 & 1-b_1 & b_1 \end{pmatrix} \begin{pmatrix} c_1 \\ 1-c_1 \\ 0 \\ 0 \end{pmatrix}, \quad \text{(B.10)}$$

$$a^{(0)} = \begin{pmatrix} a_1 \\ a_2 \\ a_3 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 1-b_1 & b_1 \\ b_1 & 0 & 0 & 1-b_1 \\ 1-b_1 & b_1 & 0 & 0 \\ 0 & 1-b_1 & b_1 & 0 \end{pmatrix} \begin{pmatrix} 1-c_1 \\ 0 \\ 0 \\ c_1 \end{pmatrix}, \quad \text{(B.11)}$$

$$a^{(0)} = \begin{pmatrix} a_1 \\ a_2 \\ a_3 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 & 1-b_1 & b_1 & 0 \\ 0 & 0 & 1-b_1 & b_1 \\ b_1 & 0 & 0 & 1-b_1 \\ 1-b_1 & b_1 & 0 & 0 \end{pmatrix} \begin{pmatrix} 0 \\ 0 \\ c_1 \\ 1-c_1 \end{pmatrix}, \quad \text{(B.12)}$$

$$a^{(0)} = \begin{pmatrix} a_1 \\ a_2 \\ a_3 \\ 0 \end{pmatrix} = \begin{pmatrix} 1-b_1 & b_1 & 0 & 0 \\ 0 & 1-b_1 & b_1 & 0 \\ 0 & 0 & 1-b_1 & b_1 \\ b_1 & 0 & 0 & 1-b_1 \end{pmatrix} \begin{pmatrix} 0 \\ c_1 \\ 1-c_1 \\ 0 \end{pmatrix}. \quad \text{(B.13)}$$

Note that (B.10), (B.11), (B.12), and (B.13) are all equivalent and they are also equivalent to

$$\begin{pmatrix} a_1 \\ a_2 \\ a_3 \end{pmatrix} = \begin{pmatrix} b_1 & 0 \\ 1-b_1 & b_1 \\ 0 & 1-b_1 \end{pmatrix} \begin{pmatrix} c_1 \\ 1-c_1 \end{pmatrix}. \quad \text{(B.14)}$$

With Proposition B.12 it follows that if $b_1, c_1 \in (0,1)$ exist, then $a_2^2 \geqslant 4a_1a_3$. Since $a_4 = 0$ and $a_1 > 0$, $a_3 > 0$, there holds $a_2^2 + a_4^2 \geqslant 4a_1a_3 > 0$.

($\Leftarrow$) Assume $a_2^2 + a_4^2 \geqslant 4a_1a_3 > 0$ and $a_4 = 0$. Then $a_2^2 \geqslant 4a_1a_3$ and from Proposition B.12 it follows that there exist $b_1, c_1 \in (0,1)$ such that (B.14) holds, from which it follows that

$$\begin{pmatrix} a_1 \\ a_2 \\ a_3 \\ 0 \end{pmatrix} = \begin{pmatrix} b_1 & 0 & 0 & 1-b_1 \\ 1-b_1 & b_1 & 0 & 0 \\ 0 & 1-b_1 & b_1 & 0 \\ 0 & 0 & 1-b_1 & b_1 \end{pmatrix} \begin{pmatrix} c_1 \\ 1-c_1 \\ 0 \\ 0 \end{pmatrix} = \operatorname{circ}(b)c$$

with $b, c \in S_+^4$ of order 2

For pattern $a^{(0)}$ the proposition has been proven. The proofs of the other patterns of a are analogously, but with (a_1, a_2, a_3) shifted. The details are omitted. □

Proposition B.15. *Let $a \in S_+^5$ be of order* 4. *Then there exist $b, c \in S_+^5$ of orders at least 2 such that $a = \operatorname{circ}(b)c$.*

Proof. It will be assumed that

$$a = \begin{pmatrix} a_1 \\ a_2 \\ a_3 \\ a_4 \\ 0 \end{pmatrix} \in S_+^5, \quad a_i > 0 \text{ for all } i \in \mathbb{Z}_4.$$

If the vector a does not have this form then there exists a transformation of a to this form, say $W_5^m a$. If it is shown that there exists b, c in S_+^5 with the necessary order properties such that $W_5^m a = \text{circ}(b)c$, then it follows that $a = \text{circ}(W_5^{5-m}b)c$. Therefore the assumption is no loss of generality.

Two cases can be distinguished depending on a property of the vector a: (1) $a_1a_4 \leqslant a_2a_3$; (2) $a_1a_4 \geqslant a_2a_3$.

Case (1): Assume that $a_1a_4 \leqslant a_2a_3$. It will be shown that there exist a $b \in S_+^5$ of order 2 or 3 and a $c \in S_+^5$ of order 2 such that

$$\begin{pmatrix} a_1 \\ a_2 \\ a_3 \\ a_4 \\ 0 \end{pmatrix} = \begin{pmatrix} b_1 & 0 & 0 & b_3 & b_2 \\ b_2 & b_1 & 0 & 0 & b_3 \\ b_3 & b_2 & b_1 & 0 & 0 \\ 0 & b_3 & b_2 & b_1 & 0 \\ 0 & 0 & b_3 & b_2 & b_1 \end{pmatrix} \begin{pmatrix} c_1 \\ c_2 \\ 0 \\ 0 \\ 0 \end{pmatrix}. \tag{B.15}$$

This equation is equivalent to

$$a_1 = b_1c_1, a_2 = b_2c_1 + b_1c_2, a_3 = b_3c_1 + b_2c_2, a_4 = b_3c_2. \tag{B.16}$$

Consider the polynomial

$$b(z)c(z) = (b_3z^2 + b_2z + b_1)(c_2z + c_1) = a_4z^3 + a_3z^2 + a_2z + a_1 = a(z).$$

Since $b_3c_2 = a_4 > 0$, assume without loss of generality that $b_3 > 0$ and $c_2 > 0$. One root of $a(z)$ is $\lambda_1 = -c_1/c_2$. Let λ_2, λ_3 denote the other roots of $a(z)$, i.e., the roots of $(b_3z^2 + b_2z + b_1)$. Then $\lambda_2 + \lambda_3 = -b_2/b_3$. Consider the Routh scheme [10], Vol. II,

$$\begin{pmatrix} a_4 & a_2 \\ a_3 & a_1 \\ a_2 - \frac{a_4}{a_3}a_1 & \\ a_0 & \end{pmatrix}.$$

It follows from Routh's criterion that all roots of $a(z)$ have negative real parts, if and only if

$$a_2 - \frac{a_4}{a_3}a_1 > 0 \quad \text{or} \quad a_1a_4 < a_2a_3.$$

So if $a_1a_4 < a_2a_3$, then $\lambda_1 < 0, Re(\lambda_2) < 0$, and $\mathrm{Re}(\lambda_3) < 0$. The consequences for b_1, b_2, and c_1 are, since $b_3 > 0$ and $c_2 > 0$:

- $\lambda_1 < 0$, if and only if $c_1/c_2 > 0$, if and only if $c_1 > 0$, if and only if $b_1 > 0$. The last equivalence follows from $c_1b_1 = a_1 > 0$.
- $\mathrm{Re}(\lambda_2) < 0$ and $\mathrm{Re}(\lambda_3) < 0$ imply $\mathrm{Re}(\lambda_2) + \mathrm{Re}(\lambda_3) = \lambda_2 + \lambda_3 < 0$, which is equivalent to $b_2/b_3 > 0$, or $b_2 > 0$.

So there exist strictly positive c_1, c_2, b_1, b_2, and b_3 such that (B.16) holds if $a_1a_4 < a_2a_3$. Since $a(1) = a_4 + a_3 + a_2 + a_1 = 1$, also $b(1)c(1) = 1$. Replacing b_i by $b_i/b(1)$ and c_i by $c_i/c(1)$, also $b(1) = b_3 + b_2 + b_1 = 1$ and $c(1) = c_1 + c_2 = 1$.

If $a_1a_4 = a_2a_3$, then a solution of (B.16) is $b_1 = a_1 + a_2$, $b_2 = 0$, $b_3 = a_3 + a_4$, $c_1 = a_1/(a_1 + a_2)$, and $c_2 = a_2/(a_1 + a_2)$.

Thus there exist $b, c \in S_+^5$ of order at least 2 such that (B.15) holds if $a_1a_4 \leqslant a_2a_3$. The proof of the second case is analogous to that of the first one, the details are omitted. □

Proposition B.16. *Let $a \in S_+^n$ be a vector of order $3 \leqslant n(a) \leqslant 4$, such that*

$$a = W_n^k \begin{pmatrix} a_1 \\ \vdots \\ a_{n(a)} \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

for some $k \in \mathbb{N}_{n-1}$, i.e., the $n(a)$ strictly positive elements are consecutive. Assume $n(a) < n$. There exist $b, c \in S_+^n$ both of order at least 2 such that

$$a = \mathrm{circ}(b)c \tag{B.17}$$

if and only if:

1. $a_2^2 \geqslant 4a_1a_3$ *for* $n(a) = 3$;
2. *always for* $n(a) = 4$, $n = 5$;
3. $a_1a_4 \leqslant a_2a_3$ *for* $n(a) = 4$, $n \geqslant 6$.

Proof. Without loss of generality it may be assumed that $k = 0$.

1. $n(a) = 3$. From Proposition A.5 it follows that $n(b) \leqslant n(a) = 3$ and $n(c) \leqslant n(a) = 3$. The possible values of the pair $(n(b), n(c))$ are $(3,3)$, $(3,2)$, $(2,3)$, $(2,2)$. The first three possibilities cannot occur as can be seen from the nonzero pattern of the vectors. So the remaining case is $(n(b), n(c)) = (2,2)$. The rest of the proof is equivalent to the proof of Proposition B.14

2. This is Proposition B.15.

3. $n(a) = 4$, $n \geqslant 6$. From Proposition A.5 it follows that $n(b) \leqslant 4$ and $n(c) \leqslant 4$. The nonzero pattern of a gives the following possible values of $(n(b), n(c))$: $(3,2), (2,3), (2,2)$. By symmetry of (B.17) in b, c it is sufficient to consider only $(3,2)$ and $(2,2)$. Assume without loss of generality that $c_1 > 0$ and $c_j > 0$ for exactly one $j \in \{2, 3, \ldots, n\}$. From Lemma B.8 it follows that if there exist $b, c \in S_+^n$ both of order at least 2 such that $a = \mathrm{circ}(b)c$, then $i(b) \subset i(a) = \{1,2,3,4\}$. For $n(b) = n(c) = 2$, possible nonzero patterns of b and c are

$$(i(b), i(c)) \in \{(\{1,2\},\{1,3\}), (\{1,3\},\{1,2\}), (\{2,4\},\{1,n\}), (\{3,4\},\{1,n-1\})\}.$$

Writing out (B.17) it follows that those patterns are possible if and only if $a_1 a_4 = a_2 a_3$.

For $n(b) = 3$, $n(c) = 2$, $(\{1,2,3\},\{1,2\})$ and $(\{2,3,4\},\{1,n\})$ are the possible nonzero patterns for $(i(b), i(c))$. The first pattern gives equations equivalent to (B.15). If $a_1 a_4 \leqslant a_2 a_3$, then from case 1 in the proof of Proposition B.15 it follows that there exists a solution. But if $a_1 a_4 > a_2 a_3$, then it follows from Routh's algorithm [10] that $a(z) = a_4 z^3 + a_3 z^2 + a_2 z + a_1$ has two roots with $\mathrm{Re}(\lambda) > 0$. The notation of the proof of Proposition B.15 will be used. If $\mathrm{Re}(\lambda_1) = -c_1/c_2 > 0$, then c_1 and c_2 cannot both be positive. So suppose $\mathrm{Re}(\lambda_2) > 0$ and $\mathrm{Re}(\lambda_3) > 0$. Then $-b_2/b_3 = \lambda_2 + \lambda_3 = \mathrm{Re}(\lambda_2) + \mathrm{Re}(\lambda_3) > 0$, so also b_2 and b_3 cannot be both positive. It follows that if $a_1 a_4 > a_2 a_3$, a cannot be written as $a = \mathrm{circ}(b)c$ with b and c of order at least 2. For the nonzero pattern $i(b) = \{2,3,4\}$ and $i(c) = \{1,n\}$ an analogous reasoning holds. □

Appendix C. Proofs for primes in the doubly stochastic matrices

C.1. Reduction of classification problem

Lemma C.1. *Let*

$$A = \sum_{i=1}^{n!} a_i P_i \in \mathrm{DS}_+^{n \times n} \tag{C.1}$$

be a doubly stochastic matrix that is not a permutation. Hence $a \in S_+^{n!}$ is a vector of order at least two. Let $L_m : S_+^{n!} \to \mathbb{R}_+^{n! \times n!}$ be the latin square induced by multiplication of the permutations, see Definition A.3.

(a) Assume that the relation between $A \in \mathrm{DS}_+^{n \times n}$ and $a \in S_+^{n!}$ according to Eq. (C.1) is a bijection. If there do not exist $b, c \in S_+^{n!}$ both of which are of order at least 2 such that

$$a = L_m(b)c \tag{C.2}$$

then $A \in \mathrm{DS}_+^{n\times n}$ defined above is a prime in the doubly stochastic matrices.

(b) If $A \in \mathrm{DS}_+^{n\times n}$ is a prime in the doubly stochastic matrices then there do not exist $b, c \in S_+^{n!}$ both of order at least 2 such that Eq. (C.2) holds.

The assumption on the bijection in Lemma C.1.a is satisfied if $A = \sum_{i\in\mathbb{Z}_n} a_i P_i$, where $\{P_i, i \in \mathbb{Z}_n\}$ is a permutation covering of $\mathbb{R}_+^{n\times n}$.

Proof of Lemma C.1. (a) Suppose that A is not a prime in the doubly stochastic matrices. Because by assumption A is not a permutation, this implies that there exist $B, C \in \mathrm{DS}_+^{n\times n}$ neither of which is a permutation such that $A = BC$. Because $B, C \in \mathrm{DS}_+^{n\times n}$, they admit the representations $B = \sum b_i P_i$ and $C = \sum c_i P_i$, for $b, c \in S_+^{n!}$. Because neither B nor C is a permutation, b, c are vectors of order at least 2. Now

$$\sum a_k P_k = A = BC = \left(\sum b_i P_i\right)\left(\sum c_i P_i\right) = \sum_k \left[\sum_{j=1}^{n!} L_m(b)_{kj} c_j\right] P_k$$

by the definition of the latin square induced by multiplication of permutations. The assumption that the relation between A and a is a bijection now implies that

$$a_k = \sum_{j=1}^{n!} L_m(b)_{kj} c_j, \quad k = 1, 2, \ldots, n!, \quad \Longleftrightarrow \quad a = L_m(b)c. \tag{C.3}$$

Then there exist $b, c \in S_+^{n!}$ of order at least 2 such that $a = L_m(b)c$. This is a contradiction of the assumption that such b, c do not exist.

(b) Suppose there do exist $b, c \in S_+^{n!}$ each of which is at least of order 2 such that $a = L_m(b)c$. Let $B = \sum b_i P_i$ and $C = \sum c_i P_i$. Then

$$BC = \left(\sum b_i P_i\right)\left(\sum c_j P_j\right) = \sum_{k=1}^{n!} \left[\sum_i \sum_{j, P_i P_j = P_k} b_i c_j\right] P_k$$

$$= \sum_{k=1}^{n!} \left[L_m(b)_{kj} c_j\right] P_k = \sum_k a_k P_k, \quad \text{by} \quad a = L_m(b)c, = A.$$

Because $b, c \in S_+^{n!}$ are of order at least 2, neither B nor C is a permutation. Then this and $A = BC$ imply that A is not a prime in the doubly stochastic matrices. This is a contradiction of the assumption. □

The classification of primes in the doubly stochastic matrices has now been reduced to the solvability of a linear equation over a latin square.

Problem C.2. Let $a \in S_+^n$ be a vector of order at least 2 and let $L : S_+^n \to \mathbb{R}_+^{n\times n}$ be the map of a doubly stochastic latin square. Determine conditions on $a \in S_+^n$ such that there do exist $b, c \in S_+^n$ both of order at least 2 such that the following equality holds

$$a = L(b)c. \tag{C.4}$$

Lemma C.3. *Let $a \in S_+^n$ be a vector of order $n(a) \geqslant 2$. Let $L : S_+^n \to \mathbb{R}_+^{n\times n}$ be the map of a latin square. There exist $b, c \in S_+^n$ both of order at least 2 such that $a = L(b)c$, iff there exist $b, c \in S_+^n$ such that $2 \leqslant n(b) \leqslant n(a)$, $2 \leqslant n(c) \leqslant n(a)$, and the following conditions both hold:*
1.

$$i(a) = \bigcup_{j\in i(c)} i(L(b)_{\cdot j}), \tag{C.5}$$

in words, the rows indexed by the strictly positive elements of the vector a equal the rows indexed by the strictly positive elements of the columns $L(b)_{\cdot j}$ for all j indexed by the strictly positive elements of the vector c;
2. and

$$a_r = L_r(b)c_r, \tag{C.6}$$

where $a_r = a|_{i(a)} \in S_+^{n(a)}$ is of order $n(a)$, $c_r = c|_{i(c)} \in S_+^{n(c)}$ is of order $n(c)$, and $L_r(b) = L(b)|_{i(a)\times i(c)}$.

Proof. ($\Leftarrow$). Let $P_1, P_2 \in P^{n\times n}$ be such that

$$P_1 a = \begin{pmatrix} a_r \\ 0 \end{pmatrix}, \quad P_2 c = \begin{pmatrix} c_r \\ 0 \end{pmatrix}.$$

Then

$$\begin{aligned} P_1 a &= \begin{pmatrix} a_r \\ 0 \end{pmatrix} = \begin{pmatrix} L_r(b) & * \\ 0 & * \end{pmatrix} \begin{pmatrix} c_r \\ 0 \end{pmatrix} \text{ by conditions 1 and 2,} \\ &= P_1 L(b) P_2^{\mathrm{T}} \begin{pmatrix} c_r \\ 0 \end{pmatrix} \text{ by condition 1} = P_1 L(b) c, \end{aligned}$$

hence $a = L(b)c$.

($\Rightarrow$). It follows from Proposition A.5 that $2 \leqslant n(b) \leqslant n(a)$ and $2 \leqslant n(c) \leqslant n(a)$. Let $P_1, P_2 \in P^{n\times n}$ be such that

$$\begin{pmatrix} a_r \\ 0 \end{pmatrix} = P_1 a, \quad \begin{pmatrix} c_r \\ 0 \end{pmatrix} = P_2 c,$$

$a_r \in S_+^{n(a)}$ and $c_r \in S_+^{n(c)}$ both of full order. Then

$$\begin{pmatrix} a_r \\ 0 \end{pmatrix} = P_1 a = P_1 L(b) P_2^{\mathrm{T}} P_2 c = \begin{pmatrix} L_r(b) & * \\ 0 & * \end{pmatrix} \begin{pmatrix} c_r \\ 0 \end{pmatrix}. \tag{C.7}$$

where the decomposition of the matrix follows form the definitions of $L_r(b)$, a_r, c_r, P_1, and P_2. That the (2,1)-block of the matrix in Eq. (C.7) is zero follows from the fact that c_r contains the strictly positive elements of the vector c. Then (C.7) implies that

$$i(a) = \bigcup_{j \in i(c)} i(L(b)_{\cdot j}) \tag{C.8}$$

and $a_r = L_r(b)c_r$. The fact that $i(a)$ indexes the strictly positive elements of the vector a implies that in (C.8) equality holds. □

C.2. *Index equations over a latin square*

In this section necessary and sufficient conditions are provided for the existence of a solution to the index equation over a latin square of Lemma C.3.

Proposition C.4. *Given* $a \in S_+^n$ with $n(a) = 2$ *and* $i(a) = (i_1, i_2)$.

(a) There exist $b, c \in S_+^n$ *with* $n(b) = n(c) = 2$ *such that* $i(a) = \cup_{k \in i(c)} i(L_m(b)_{\cdot k})$ *iff* $P_{i_1} P_{i_2}^{\mathrm{T}} = P_{i_2} P_{i_1}^{\mathrm{T}}$.

(b) If the condition of a holds then all solutions are given by

$$P_{j_1} \in P^{n \times n} \text{ arbitrary}, \quad P_{j_2} = (P_{i_1} P_{i_2}^{\mathrm{T}}) P_{j_1}, \quad P_{k_1} = P_{j_1}^{\mathrm{T}} P_{i_1}, \quad P_{k_2} = P_{j_1}^{\mathrm{T}} P_{i_2},$$
$$i(b) = (j_1, j_2), \quad i(c) = (k_1, k_2).$$

Proof. Suppose that $b, c \in S_+^n$ exist. Let $i(b) = (j_1, j_2)$ and $i(c) = (k_1, k_2)$. Then the index relation holds iff, case 1,

$$L_m(b)_{i_1,k_1} = b_{j_1}, \quad L_m(b)_{i_1,k_2} = b_{j_2}, \quad L_m(b)_{i_2,k_1} = b_{j_2}, \quad L_m(b)_{i_2,k_2} = b_{j_1},$$

or, case 2, the assignment with the indices j_1 and j_2 interchanged holds. In case 1 there follows from the definition of L_m that the relations equal

$$P_{j_1} P_{k_1} = P_{i_1}, \quad P_{j_2} P_{k_1} = P_{i_2}, \quad P_{j_2} P_{k_2} = P_{i_1}, \quad P_{j_1} P_{k_2} = P_{i_2}.$$

From this follows that

$$P_{k_1} = P_{j_1}^{\mathrm{T}} P_{i_1} = P_{j_2}^{\mathrm{T}} P_{i_2}, \quad P_{k_2} = P_{j_2}^{\mathrm{T}} P_{i_1} = P_{j_1}^{\mathrm{T}} P_{i_2}, \quad P_{j_2} = P_{i_1} P_{k_2}^{\mathrm{T}} = P_{i_1} P_{i_2}^{\mathrm{T}} P_{j_1}, \tag{C.9}$$
$$P_{i_1} P_{i_2}^{T} = P_{j_1} P_{j_2}^{\mathrm{T}} = P_{i_2} P_{i_1}^{\mathrm{T}}. \tag{C.10}$$

In case 2 the same conclusion results. Part (b) follows immediately from (C.9). □

Example C.5. Let $a \in S_+^6$ with $n(a) = 2$ and $i(a) = (i_1, i_2)$. For which tuples $(i_1, i_2) \subset \mathbb{Z}_6$ do there *not* exist $b, c \in S_+^6$ with $n(b) = 2 = n(c)$ such that $i(a) = \cup_{k \in i(c)} i(L_m(b)_{,k})$. According to Proposition C.4 such b, c do not exist iff $P_{i_1} P_{i_2}^{\mathrm{T}} \neq P_{i_2} P_{i_1}^{\mathrm{T}} = P_x$. The only possible choices for $P_x \in P^{6\times 6}$ such that $P_x \neq P_x^{\mathrm{T}}$ are $P_x = P_2$ and $P_x = P_3$. From $P_x = P_{i_2} P_{i_1}^{\mathrm{T}}$ follows $P_{i_2} = P_x P_{i_1}$. For $P_x = P_2$ the possible tuples (i_1, i_2) are $(1,2)$, $(2,3)$, $(3,1)$, $(4,6)$, $(5,4)$, and $(6,5)$. For $P_x = P_3$ one obtains the same tuples. Because the ordering of i_1 and i_2 is unimportant the tuples may also be written as $(1,2)$, $(2,3)$, $(1,3)$, $(4,5)$, $(4,6)$, and $(5,6)$.

Proposition C.6. *Let $a \in S_+^n$ with $n(a) = 3$ and $i(a) = (i_1, i_2, i_3) \subset \mathbb{Z}_n$.*

(a) There exist $b, c \in S_+^n$ both of order 2 such that

$$i(a) = \cup_{k \in i(c)} i(L_m(b)_{,k}) \tag{C.11}$$

iff one of the following three conditions holds:

$$P_{i_1} P_{i_2}^{\mathrm{T}} = P_{i_2} P_{i_3}^{\mathrm{T}}, \quad P_{i_1} P_{i_2}^{\mathrm{T}} = P_{i_3} P_{i_1}^{\mathrm{T}}, \quad P_{i_3} P_{i_1}^{\mathrm{T}} = P_{i_2} P_{i_3}^{\mathrm{T}}. \tag{C.12}$$

(b) If one of the conditions of (a) holds then all combinations of the indices of b, c are constructed as follows, in case $P_{i_1} P_{i_2}^{\mathrm{T}} = P_{i_2} P_{i_3}^{\mathrm{T}}$:

$$P_{j_1} \in P^{n\times n} \text{ arbitrary}, \quad P_{j_2} = (P_{i_2} P_{i_1}^{\mathrm{T}}) P_{j_1}, \quad P_{k_1} = P_{j_1}^{\mathrm{T}} P_{i_1}, \quad P_{k_2} = P_{j_2}^{\mathrm{T}} P_{i_3},$$
$$i(b) = (j_1, j_2), \quad i(c) = (k_1, k_2).$$

The solution in the other cases is easily deduced by symmetry.

The proof of Proposition C.6 is easily deduced from that of Proposition C.4. The same holds for the following results.

Proposition C.7. *Let $a \in S_+^n$ with $n(a) = 3$ and $i(a) = (i_1, i_2, i_3) \subset \mathbb{Z}_n$. There exist $b, c \in S_+^n$ with $n(b) = 3$ and $n(c) = 2$ such that Eq. (C.11) holds iff*

$$P_{i_1} P_{i_2}^{\mathrm{T}} = P_{i_2} P_{i_3}^{\mathrm{T}} = P_{i_3} P_{i_1}^{\mathrm{T}}. \tag{C.13}$$

Proposition C.8. *Let $a \in S_+^n$ with $n(a) = 3$ and $i(a) = (i_1, i_2, i_3) \subset \mathbb{Z}_n$.*

(a) There exist $b, c \in S_+^n$ with $n(b) = 3$ and $n(c) = 3$ such that Eq. (C.11) holds iff

$$P_{i_1} P_{i_2}^{\mathrm{T}} = P_{i_2} P_{i_3}^{\mathrm{T}} = P_{i_3} P_{i_1}^{\mathrm{T}}. \tag{C.14}$$

(b) Assume that the condition of (a) holds. All solutions for b, c are constructed by:

$$P_{j_1} \in P^{n\times n} \text{ arbitrary}, \quad P_{j_2} = P_{i_2} P_{i_1}^{\mathrm{T}} P_{j_1}, \quad P_{j_3} = P_{i_1} P_{i_2}^{\mathrm{T}} P_{j_1}, \quad P_{k_1} = P_{j_1}^{\mathrm{T}} P_{i_1},$$
$$P_{k_2} = P_{j_1}^{\mathrm{T}} P_{i_2}, \quad P_{k_3} = P_{j_1}^{\mathrm{T}} P_{i_3}, \quad i(b) = (j_1, j_2, j_3), \quad i(c) = (k_1, k_2, k_3).$$

Lemma C.9. *Let $a \in S_+^n$ with $n(a) = 3$ and $i(a) = (i_1, i_2, i_3) \subset \mathbb{Z}_n$.*

(a) There exist $b, c \in S_+^n$ both of order at least 2 such that Eq. (C.11) holds iff of the three products $P_{i_1}P_{i_2}^{\mathrm{T}}$, $P_{i_2}P_{i_3}^{\mathrm{T}}$, $P_{i_3}P_{i_1}^{\mathrm{T}}$ two are equal or all three are equal.

(b) The conditions of Part (a) remain the same if the order of the indices in $i(a) = (i_1, i_2, i_3)$ is arbitrarily interchanged.

Proof. ($\Rightarrow$) If $b, c \in S_+^n$ exist then it follows from Eq. (C.11) that $2 \leqslant n(b) \leqslant n(a) = 3$ and the same bounds on $n(c)$. The possible values of $(n(b), n(c))$ are thus $(2,2)$, $(2,3)$, $(3,2)$, and $(3,3)$. The result then follows from the three previous propositions.

($\Leftarrow$) This follows from the three previous propositions. □

Proposition C.10. *Let $a \in S_+^6$ be of order 3 with $i(a) = (i_1, i_2, i_3) \subset \mathbb{Z}_6$. There exist $b, c \in S_+^6$ both of order at least 2 such that Eq. (C.11) holds iff either $i(a) = (1,2,3)$ or $i(a) = (4,5,6)$.*

Proof. Lemma C.9 is applied. For $i(a) = (1,2,3)$ the products are all equal to P_3 while for $i(a) = (4,5,6)$ they are all equal to P_2. All other ordered triples in $\mathbb{Z}_6$ with different elements are: $(1,2,4)$, $(1,2,5)$, $(1,2,6)$, $(1,3,4)$, $(1,3,5)$, $(1,3,6)$, $(1,4,5)$, $(1,4,6)$, $(2,3,4)$, $(2,3,5)$, $(2,3,6)$, $(2,4,5)$, $(2,4,6)$, $(2,5,6)$, $(3,4,5)$, $(3,4,6)$, and $(3,5,6)$. For $i(a) = (1,2,5)$, $P_1P_2^{\mathrm{T}} = P_3$, $P_2P_5^{\mathrm{T}} = P_4$, $P_5P_1^{\mathrm{T}} = P_5$ hence the three products are different. Similarly in all other cases the three products are each different. □

C.3. Specific linear equations over a doubly stochastic latin square

Example C.11. Let $a \in S_+^2$ be of order 2. Do there exist $b, c \in S_+^2$ of order at least 2 such that $a = L_m(b)c$? In this case, because of the dimensions of the vectors involved, $L_m(b) = \mathrm{circ}(b)$. The existence of b and c then follows from the Propositions B.2 and B.5.

The next result is a specific case of Problem C.2.

Proposition C.12. *Let $a \in S_+^{3!} = S_+^6$ be of order 2. Then there do not exist $b, c \in S_+^6$ both of order at least 2 such that*

$$a = L_m(b)c \tag{C.15}$$

iff the indices of the strictly positive elements of the vector a are given by

$$i(a) = (1,2),\ (1,3),\ (2,3),\ (4,5),\ (4,6),\ \text{or}\ (5,6). \tag{C.16}$$

Note that the values of the strictly positive components of the vector a are unconstrained.

Proof. By Lemma C.3 there exist $b, c \in S_+^6$ both of order at least 2 such that Eq. (C.15) holds iff

$$i(a) = \bigcup_{j \in i(c)} i(L_m(b)_{\cdot j}). \tag{C.17}$$

$$a|_{i(a)} = L_m(b)|_{i(b) \times i(c)} c|_{i(c)}. \tag{C.18}$$

From Example C.11 follows that Eq. (C.18) always has a solution. By Proposition C.4 and Example C.5 there do not exist solutions b, c of (C.17) iff the index set $i(a)$ is one of the cases mentioned in Eq. (C.16). □

Proposition C.13. *Let $a \in S_+^n$ be of order 2 with $i(a) = (i_1, i_2) \subset Z_n$, $i_1 \neq i_2$. Then there do exist $b, c \in S_+^n$ both of order at least 2 such that $a = L_m(b)c$ iff*

$$P_{i_1} P_{i_2}^{\mathrm{T}} = P_{i_2} P_{i_1}^{\mathrm{T}}. \tag{C.19}$$

Proof. From Proposition A.5 follows that if there exist $b, c \in S_+^n$ satisfying $a = L_m(b)c$ both of order at least 2 then both b and c are of order at most 2, hence precisely 2. From Lemma C.3 follows that there exist $b, c \in S_+^n$ both of order 2 such that $a = L_m(b)c$ iff Eqs. (C.5) and (C.6) both hold with $L = L_m$. From Proposition C.4 follows that Eq. (C.5) holds iff Eq. (C.19) holds. From Example C.11 follows that in this case Eq. (C.6) always has a solution. □

Proposition C.14. *Let $a \in S_+^6$ be of order 3. There do exist $b, c \in S_+^6$ both of order at least 2 such that $a = L_m(b)c$ iff either $i(a) = (1, 2, 3)$ or $i(a) = (4, 5, 6)$.*

Proof. From Lemma C.3 follows that $b, c \in S_+^6$ as formulated in the statement of the proposition do exist iff Eqs. (C.5) and (C.6) both hold with $L = L_m$. From Proposition C.10 follows that Eq. (C.5) has a solution iff $i(a) = (1, 2, 3)$ or $i(a) = (4, 5, 6)$. If $i(a) = (1, 2, 3)$ then it follows from Proposition C.8 that $i(c) = (1, 2, 3)$ and hence the Equation $a_r = L_r(b)c_r$ reduces to

$$\begin{pmatrix} a_1 \\ a_2 \\ a_3 \end{pmatrix} = \operatorname{circ} \begin{pmatrix} b_1 \\ b_2 \\ b_3 \end{pmatrix} \begin{pmatrix} c_1 \\ c_2 \\ c_3 \end{pmatrix}. \tag{C.20}$$

It then follows from Propositions B.2 and B.5 that this equation has a solution. If $i(a) = (4, 5, 6)$ then a permutation must be applied to transform Eq. (C.6) to the form of Eq. (C.20). Thus in this case Eq. (C.6) also has a solution. □

References

[1] A. Berman, M. Neumann, R.J. Stern, Nonnegative Matrices in Dynamic Systems, Wiley, New York, 1989.
[2] A. Berman, R.J. Plemmons, Nonnegative Matrices in the Mathematical Sciences, Academic Press, New York, 1979.
[3] A. Berman, R.J. Plemmons, Nonnegative matrices in the mathematical sciences, Number 9 in Classics in Applied Mathematics, SIAM, Philadelphia, 1993.
[4] R.A. Brualdi, S.V. Parter, H. Schneider, The diagonal equivalence of a nonnegative matrix to a stochastic matrix, J. Math. Anal. Appl. 16 (1966) 31–50.
[5] R.A. Brualdi, H.J. Ryser, Combinatorial Matrix Theory, Cambridge University Press, Cambridge, 1991.
[6] P.J. Davis, Circulant Matrices, Wiley, New York, 1979.
[7] D. de Caen, D.A. Gregory, Primes in the semigroup of boolean matrices, Linear Algebra Appl. 37 (1981) 119–134.
[8] J. Dénes, A.D. Keedwell, Latin Squares: New Developments in the Theory and Applications, North-Holland, Amsterdam, 1991.
[9] J. Dieudonné, Foundations of Modern Analysis, Academic Press, New York, 1969.
[10] F.R. Gantmacher, The Theory of Matrices, vols. 1/2, Chelsea, New York, 1959.
[11] J.S. Golan, The Theory of Semirings with Applications in Mathematics and Theoretical Computer Science, Longman, Harlow, 1992.
[12] N. Jacobson, Basic Algebra, vols. 1/2, 2nd edn., Freeman, New York, 1985.
[13] M. Lewin, On nonnegative matrices, Pacific J. Math. 36 (1971) 753–759.
[14] D. London, On matrices with a doubly stochastic pattern, J. Math. Anal. Appl. 34 (1971) 648 652.
[15] M. Marcus, K. Kidman, M. Sandy, Products of elementary doubly stochastic matrices, Linear and Multilinear Algebra 15 (1984) 331–340.
[16] A.W. Marshall, I. Olkin, Inequalities: Theory of Majorization and its Applications, Academic Press, New York, 1979.
[17] H. Minc, Nonnegative Matrices, Wiley, New York, 1988.
[18] L. Mirsky, Results and problems in the theory of doubly stochastic matrices, Z. Wahrscheinlichkeitstheorie 1 (1963) 319–334.
[19] B.N. Parlett, T.L. Landis, Methods for scaling to doubly stochastic form, Linear Algebra Appl. 48 (1982) 53–79.
[20] H. Perfect, L. Mirsky, The distribution of positive elements in doubly stochastic matrices, J. London Math. Soc. 40 (1965) 689–698.
[21] G. Picci, J.H. van Schuppen, Stochastic realization of finite-valued processes and primes in the positive matrices, in: H. Kimura, S. Kodama (Eds.), Recent advances in mathematical theory of systems, control, networks, and signal processing II, Proceedings of the International Symposium MTNS-91, Mita Press, Tokyo, 1992, pp. 227–232.
[22] D.J. Richman, H. Schneider, Primes in the semigroup of non-negative matrices, Linear and Multilinear Algebra 2 (1974) 135–140.